LUISS Guido Carli
LIBERA UNIVERSITA' INTERNAZIONALE DEGLI STUDI SOCIALI

Dipartimento di Giurisprudenza

A. A. 2013/14

Tesi in Diritto Penale 2

LA TUTELA PENALE DELLA PRIVACY

RELATORE:

Chiar.mo Prof. Maurizio Bellacosa

CANDIDATO: Ettore Corsini

MATR.: 100023

CORRELATORE:

Chiar.ma Prof.ssa Elisa Scaroina

INDICE

CAPITOLO IV – I REATI PRIVACY IMPROPRI: IL CODICE PENALE

CAPITOLO V – I REATI A TUTELA DELLA PRIVACY E LA DISCIPLINA DELLA RESPONSABILITÀ DEGLI ENTI

CAPITOLO I – L'EVOLUZIONE STORICA E NORMATIVA IN MATERIA DI PRIVACY

1. Premessa storica al concetto di privacy - 2. Le origini americane: Warren & Brandeis - 3. Privacy e Costituzione americana, il Quarto Emendamento e le prime affermazioni giurisprudenziali e dottrinali sulla privacy - 4. Il riconoscimento del diritto alla privacy all'interno dei diritti della personalità in Europa - 5. Le posizioni della dottrina e della giurisprudenza italiana prima delle leggi sulla privacy: il bene giuridico nella Costituzione - 6. La direttiva 95/46/CE e la L. 675/96 - 7. Il Codice della Privacy: D.lgs 196/2003

1. Premessa storica al concetto di privacy

Il termine privacy, utilizzato in italiano anche col corrispettivo riservatezza[1], sebbene come concetto sociologico possa considerarsi di semplice ed immediata captazione all'individuo comune, in virtù dei suoi risvolti principalmente informatici che coinvolgono oggi giorno chiunque interagisca in modo preponderante con strumenti quali internet, computers, smartphones e via dicendo, nasconde in realtà un evoluzione non solo storico-giuridica, ma anche, per l'appunto, storico-sociale, che infonde le sue radici in epoche molto antiche.

Polis e Oikos: la nascita del concetto in antica Grecia

Probabilmente, la posizione più autorevole è rinvenibile nell'antica Grecia da parte del celebre filosofo di Stagira. Aristotele propone, in una delle sue opere[2] più illustri, una distinzione ormai classica fra la sfera pubblica, connessa all'attività politica intesa col corrispondente greco di *Polis*, e la sfera privata, *Oikos*, associata alla famiglia ed alla vita domestica. In questo modo viene individuato un ambito personale e familiare come un entità distaccata ma

[1] Questa posizione tuttavia non è pacifica. Dal punto di vista prettamente linguistico, riservatezza è tradotto in inglese come *confidentiality*, intendendolo in modo più ampio del termine *privacy*. Dal punto di vista giuridico invece spesso si parla di privacy, riservatezza e tutela dei dati personali come sinonimi. Tuttavia, come si vedrà nel corso di quest'elaborato, è più corretto considerarli come fossero facciate della stessa piramide piuttosto che come semplici significati equivalenti.

[2] ARISTOTELE, *La politica,* Le Monnier, Firenze, 1981.

soprattutto tutelata rispetto all'ambito pubblico e politico dalla quale si comincia a prendere le distanze.

Sulle stesse note di questa posizione, sempre in Grecia, anche il celeberrimo drammaturgo ateniese, Sofocle, propone nell'Antigone [3], in modo sorprendentemente attuale, una netta distinzione fra sfera pubblica e sfera privata, che si ripercuote alla luce della distinzione fra diritto positivo e diritto naturale. Questa tragedia[4] rappresenta un vero e proprio punto di partenza non solo sociale ma anche giuridico per l'affermazione della libertà personale alla luce del diritto naturale opposto alle ferree leggi dello Stato del diritto positivo.

È per codesto motivo che questa affermazione, lontana ben più di due millenni dalle vicende greche ora trattate, suona invece come fortemente familiare in relazione all'opposizione sopra citata.

Le origini moderne: Inghilterra

"Every man's home is his castle"[5], così William Pitt, Conte di Chatham, esordisce nel 1763 in un discorso alla Camera dei Lord per sviluppare poi un efficace metafora che fornisce la visione della privacy nell'Europa illuminista e pre-rivoluzionaria. Queste le sue parole: "*il più povero degli uomini può, nella sua casetta, lanciare una sfida opponendosi a tutte le forze della corona. La casetta può essere fragile, il suo tetto può essere traballante, il vento può soffiare da tutte le parti, la tempesta può entrare e la pioggia può entrare, ma il Re d'Inghilterra non può entrare: tutte le sue forze non osano attraversare la soglia di tale casetta in rovina"*[6]. Tuttavia, nonostante le ardenti parole di

[3] SOFOCLE, *Edipo re – Edipo a Colono – Antigone*, a cura di Dario Del Corno, Oscar Mondadori, 2006.

[4] Tale opera, forse punta di diamante fra le tragedie sofoclee, racconta la storia di Antigone, che decide di dare sepoltura al cadavere del fratello Polinice contro la volontà del nuovo re di Tebe, Creonte. Scoperta, viene condannata dal re a vivere il resto dei suoi giorni imprigionata in una grotta, nella quale poi si impicca. Questo porta al suicidio del figlio di Creonte, Emone (promesso sposo di Antigone), e poi della moglie di Creonte, Euridice, lasciando il solo Creonte a maledire la propria stoltezza. Le azioni della protagonista, che nascono nella sua coscienza come diritto naturale si contrappongono alle leggi positive di Creonte che negano la sepoltura del fratello così come la sfera privata dell'O*ikos* comincia a staccarsi dalla sfera pubblica della P*olis* greca.

[5] La casa di ogni uomo è il suo castello.

[6] PITT W., The Elder, Lord Chatham, discorso del Marzo 1763, citato in Henry Peter Brougham, *Historical Sketches of statesmen Who Flourished in the Time of George III*, Charles Knights & Co, Londra, 1839, vol. 1.p. 52: "*The poorest man may in his cottage bid defiance to all the forces of the*

William Pitt, che ritraggono i limiti all'azione dello Stato e della sfera pubblica nei confronti dell'individuo, il concetto (ed il diritto) di privacy, all'interno di quest'epoca storica rimane ancora difficilmente delineabile sotto il punto di vista del bene protetto del diritto stesso. La posizione del Conte di Chatham, infatti, dipinge il diritto alla privacy come un diritto di ogni individuo, un diritto universale, ma, purtroppo, non è questo il punto di partenza accolto in età moderna poiché, come a breve vedremo, esso nasce in realtà come un diritto dei pochi e, soprattutto, dei ricchi, mutuato sulla logica proprietaria di stampo ottocentesco.

Il problema di una definizione univoca

Prima di poterne raggiungere una concezione soddisfacente e sufficientemente attuale, bisognerà ripercorrere lo sviluppo dottrinale e giurisprudenziale del concetto, partendo dall'esperienza americana, passando per il famoso manifesto sul diritto alla privacy di Warren e Brandeis e per le vicende legate al Quarto Emendamento della Costituzione americana, per poi approdare in Europa e sviluppare l'evoluzione ed il riconoscimento di questo diritto sull'intero continente fino a giungere, nel nostro Paese, alle prime affermazioni giurisprudenziali ed alle successive leggi in materia di riservatezza a traduzione delle discipline sviluppatesi in ambito europeo.

Fin da subito bisogna comunque precisare che difficilmente è ricostruibile un concetto certo, ben delineato ma soprattutto univoco di privacy non solo dal punto di vista giuridico ma anche storico-sociale, dal momento che, in virtù di ogni periodo storico, esso è soggetto a differenti compressioni o amplificazioni.

L'innovativa definizione di Alan Westin

A conclusione di questo rapido *incipit* storico, proprio per esprimere la forte difficoltà di molti autori e studiosi ad accordarsi su un'unica definizione di tale concetto è utile richiamare la posizione di Alan Westin[7] che, nel suo libro

---

Crown. It may be frail—its roof may shake—the wind may blow through it—the storm may enter—the rain may enter—but the King of England cannot enter!—all his force dares not cross the threshold of the ruined tenement!".

[7] Professore di Diritto Pubblico presso la Columbia University di New York, considerato ad oggi uno dei più grandi esperti di privacy negli Stati Uniti.

Privacy and Freedom[8], ammette che "*pochi valori cosi fondamentali per la società sono talmente indefiniti negli studi sociali o sono stati così vaghi ed indefiniti negli scritti degli esperti di teoria sociale"*[9]. Successivamente, cercando comunque di delineare dei confini al valore della riservatezza, fornisce una definizione molto attuale, spezzando le catene di quella posizione ottocentesca imperniata sul modello giuridico della proprietà privata, per la quale *"la privacy è riconosciuta pienamente come diritto e anche potere che scaturisce da un insindacabile atto di volontà. È una pretesa legittima che ogni individuo ha di decidere in che misura e in che modo vuole condividere una parte di sé con gli altri. Privacy è sinonimo del diritto d'essere lasciato solo, definita anche come relazione zero fra due o più persone nel senso che non c'è interazione fra loro se decidono così. Ma l'uomo vive in una comunità ed ha anche la necessità di partecipare e comunicare dunque quando questo aspetto della privacy a due lati si scontra col potere riconosciuto del governo di funzionare per il benessere pubblico, ben si motiva la problematica recente sulle invasioni e intrusioni nella privacy individuale"*[10].

Tuttavia, come accennato poc'anzi, un risultato del genere sarà raggiunto solo a seguito di un'evoluzione costante, durata quasi due secoli, a cavallo del nuovo e del vecchio continente.

[8] WESTIN A., *Privacy and Freedom,* Atheneum, New York, 1970, pag. 1.

[9] *"Few values so fundamental to society have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists.*

[10] *"Privacy is the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place and circumstances to communicate to others. Privacy is synonymous with the right to be let alone, also defined as a "zero-relationship" between two or more persons in the sense that there is no interaction between them if they so choose. But man lives in community of others, and he also has the need to participate and communicate. When this double-faceted aspect of privacy is coupled with the recognized power of government to function for the public good, there is ample reason for much of the recent concern about invasion and intrusions into individual privacy."*

2. Le origini americane: Warren & Brandeis

La nascita dell'espressione "Right to be let alone"

Come condiviso da diversi Autori[11], storicamente il diritto alla privacy, inteso, dal punto di vista squisitamente giuridico, nacque connaturatamente alla famosa espressione *"the right to be let alone"*[12], famosa almeno quanto i giuristi stessi che la coniarono, nel 1890, all'interno del saggio *The Right to Privacy*[13]che ebbe il merito di avviare una vera e propria rivoluzione giuridica e sistematica sul concetto di privacy e che a breve sarà trattata approfonditamente.

In realtà non furono proprio Warren e Brandeis i primi a porsi il problema di una tutela della privacy nei confronti dell'individuo. Infatti, da un punto di vista prettamente temporale, nel 1888 fu il giudice Thomas Cooley[14] ad analizzare preliminarmente la questione. Egli, in un saggio sugli illeciti extracontrattuali[15], rintracciò l'esistenza di un diritto alla privacy come funzionale alla sicurezza personale; non ne fu un'analisi diretta bensì, in un certo senso, casuale, dal momento che l'analisi primaria era indirizzata su un tema diverso. Tuttavia fu proprio il giudice Cooley a coniare per la prima volta l'interessante formula sopra citata, diventata poi tanto cara alla dottrina e alla giurisprudenza successiva in tutto il mondo.

Il saggio di Warren e Brandeis

Tornando ai due giuristi del Massachussets, il loro saggio nacque a seguito di una vicenda strettamente personale riguardante la vita matrimoniale dello stesso Warren[16] che fu pubblicata da uno dei primi giornali ad utilizzare la stampa a rotativa, la *Boston Evening Gazette*, e che quindi permise la

[11] Uno su tutti: RODOTA' S., *Intervista su privacy e libertà,* a cura di Paolo Conti, Editori Laterza, Roma-Bari, 2005, p. 8.
[12] *"Il diritto ad essere lasciati in pace".*
[13] BRANDEIS L.D., WARREN S., *The Right to Privacy,* in 4 Harward Law Review, 1890, pp 193-220.
[14] Trattasi del giudice supremo della suprema corte del Michigan, fra il 1864 ed il 1885.
[15] COOLEY T.C., *A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract,* Callaghan & Company, Chicago, IL, 1888, p. 29. In realtà la citazione *"the right to be let alone"* è tratta dalla prefazione alla seconda edizione dell'opera di Cooley, che fu scritta ancor prima, nel 1879 in seguito ad un caso giurisprudenziale riscontrato dallo stesso giudice supremo.
[16] Si trattava di indiscrezioni piccanti relative alla moglie, o alla figlia, a seconda degli autori del tempo, del giurista.

conoscenza e la diffusione dell'argomento ad un elevata mole (per quei tempi) di persone. Tale questione fu lo spunto che mosse i giuristi a interrogarsi profondamente sino a che punto fosse possibile, tramite i nuovi strumenti tecnici dell'epoca, divulgare informazioni personali al pubblico così da violarne la riservatezza. Giunsero quindi a rintracciare un vero e proprio nuovo diritto della persona (*Right to privacy)* definito come *"right to be let alone"*[17]*,* sviluppatosi in virtù dei cambiamenti politici, sociali, economici della società americana di fine secolo: a conclusione di questo elaborato giuridico pubblicarono un saggio, nel 1890, denominato proprio *Right to Privacy.*

Fortemente i due giuristi sottolinearono quanto importante fosse il mutamento tecnologico[18], e quanto esso fosse l'elemento principale a rendere necessaria una rinnovata riflessione più specifica e attenta sui diritti del singolo.

Privacy negativa intesa nella logica della proprietà privata

Venendo al significato più profondo attribuito a questo diritto, Warren e Brandeis asserivano che si trattasse di un concetto rintracciabile all'interno di un principio già insito al sistema di Common Law che andava a tutelare l'area privata del singolo, inteso come quello spazio domestico nel quale ognuno poteva fare quel che desiderava, pensare senza ingerenze, al riparo da occhi ed orecchie altrui.

Si trattava dell'istituto giuridico della proprietà privata, inteso a quell'epoca, secondo una concezione molto in voga e cara al modello liberale, come l'apposizione di chiusure e steccati per non permettere agli altri di subentrare nel proprio terreno, espresso col termine latino "*ius excludendi alios"*. In questo modo, per gli autori, il diritto alla privacy è un concetto essenziale che

[17] Nuovamente, come per il caso del giudice Cooley, non si vuole certo dire che il concetto *"right to be let alone"* non fosse mai stato utilizzato, ma che mai fosse stato inteso in maniera così vincolata come alla base di un nuovo e rivoluzionario diritto: quello alla riservatezza. Di fatti, il termine è stato utilizzato ad esempio in *Wheaton vs. Peters,* 33 U.S. 591,634, 1834, in Ronald B. Standler, *Privacy Law in the U,S,A,*1997; si tratta di una sentenza della Corte Suprema americana nella quale fu sancito in pieno il diritto dell'imputato ad essere lasciato in pace fino a che non fosse stato provato che avesse violato il diritto di un altro soggetto.

[18] Ovviamente, anche il contesto storico non è casuale: la nascita della stampa a rotativa, della fotografia moderna e via dicendo, sono causa della forte rivoluzione industriale del XIX secolo, propria di un balzo verso la modernità senza precedenti e figlia, a sua volta,delle rivoluzioni a cavallo fra il XVIII ed il XIX secolo.

sottace alla ricerca della felicità, riconosciuto come diritto fondamentale della cultura statunitense, nonché baluardo della stessa Costituzione Americana.

È evidente come, cosi delineato, il concetto di privacy assume una componente completamente negativa, intesa come quel diritto di non voler intrusioni nella propria sfera privata, così come in parte intendeva William Pitt nel discorso alla Camera dei Lord del 1763.

Il problema dell'influenza della classe sociale

In realtà è presente una profonda differenza che allontana il saggio di Warren e Brandeis dalla posizione del Conte di Chatam, e che lo tiene distante, a sua volta, da tutte le posizioni future che si sviluppano sul concetto in questione.

Trattasi del fatto che il diritto alla riservatezza inteso nel saggio *The Right to Privacy* è costruito con prevalente riferimento alla figura del quale classe sociale medio-alta all'interno dei ceti sociali dell'epoca.

La rivoluzione tecnologica, dal punto di vista della tutela della riservatezza, colpì quasi esclusivamente la classe aristocratica che, a quel tempo, si sentiva ancora legata ad un forte sentimento di intangibilità nei confronti delle classi sociali inferiori e che dunque poteva ritenersi offesa da violazioni alla loro privacy al contrario di quest'ultime. Non è un caso se il problema è sollevato proprio da due giuristi, appartenenti ad un ceto eminentemente aristocratico; se non fossero stati professionisti affermati, il successo del loro articolo non sarebbe certo stato di tale portata.

In questo senso, il diritto alla privacy sebbene nasca nell'epoca borghese, si origina come un diritto dei ricchi, degli aristocratici, di quel ceto descritto come "*ancien régime"*. In realtà, come vedremo a breve, sarà proprio Brandeis [19] (e non Warren) a far evolvere ulteriormente il diritto alla riservatezza ad un livello successivo, così da scavalcare nuovamente quelle catene e consentire progressivamente il raggiungimento di un nuovo e più ampio livello di tutela.

[19] Infatti, sebbene Brandeis e Warren vengano ricordati entrambi per il loro apporto sul tema qui trattato, solo Brandeis rimane anche in seguito al centro del dibattito sul diritto alla riservatezza, tanto da diventare addirittura giudice di Corte Suprema, approfondendo ulteriormente il tema della rilevanza dell'evoluzione tecnologica in contrapposizione all'individuo.

3. *Privacy e Costituzione americana, il Quarto Emendamento e le prime affermazioni giurisprudenziali e dottrinali sulla privacy*

La Costituzione Americana, legge suprema degli Stati Uniti d'America, fu ufficialmente completata il 17 settembre del 1787 e, nel corso dei due anni successivi, venne progressivamente ratificata tramite particolari Convenzioni da parte dei tredici Stati esistenti all'epoca, di modo che nel 1789 entrò in vigore sul territorio nazionale. Essa pone le sue radici nella lontana Magna Charta britannica del 1215 e nel *Bill of Rights*[20], che aggiunse Dieci Emendamenti nel 1791. Tuttavia, in un primo momento, l'applicazione di questi Emendamenti era circoscritta ai cittadini americani esclusi gli abitanti della Virginia e dello stato di New York, questo perché in tali luoghi le leggi statali potevano ancora prevalere sulla Costituzione Americana.

Il Quarto Emendamento della Costituzione Americana

Solo nel 1868, con l'introduzione del Quattordicesimo Emendamento[21], fu proibito ai vari di Stati di varare leggi contrarie alla Costituzione e dunque solo da quel momento fu estesa alla totalità dei cittadini americani la possibilità di vedersi applicati tutti i diritti sanciti dal *Bill of Rights*.

All'interno di questa Carta, è di fondamentale importanza, per il nostro studio, il Quarto Emendamento. Esso non prevede un espresso riferimento al diritto alla privacy nei confronti del cittadino americano, tuttavia, ciò non impedisce comunque di ritenere che la privacy sia un bene giuridico costituzionalmente tutelato. "*Il diritto dei cittadini ad essere assicurati nelle loro persone, case, carte ed effetti contro perquisizioni e sequestri non ragionevoli, non potrà essere violato, e non potranno essere emessi mandati se non su motivi*

[20] Si tratta per l'appunto di un documento contenente i primi dieci emendamenti della Costituzione Americana; furono introdotti da parte di James Madison, riconosciuto come uno dei "*fathers of constitution"* e quarto Presidente degli Stati Uniti d'America. Furono stilati prendendo spunto dalla Dichiarazione dei Diritti proclamata in Virginia, nel 1776.

[21] Quest'emendamento fu ratificato il 9 luglio del 1868 e, non a caso, è figlio delle appena trascorse guerre di secessione; è costruito attorno alla definizione della "cittadinanza", il principale scopo dell'emendamento fu infatti di escludere schiavi e loro discendenti dai diritti costituzionali e di parificare i diritti dei cittadini americani alla Costituzione introducendo la cd. clausola di uguale protezione, di modo che nessuna legge federale potesse sovrapporsi ai dettati costituzionali.

probabili, sostenuti da giuramenti o solenni affermazioni e con una dettagliata descrizione del luogo da perquisire e delle persone o cose da prendere in custodia"[22]. Come è evidente, manca un espresso riferimento ad un diritto alla riservatezza nel menzionato Emendamento, tuttavia, agli occhi di un lettore moderno, non è certo possibile non rintracciare almeno una scia, un sentore, del concetto di privacy quantomeno a livello embrionale.

La dissenting opinion del giudice Brandeis in Olmstead Vs. United States

Probabilmente, uno dei primi giuristi ad accogliere una lettura moderna di questo tipo, fu proprio Luis Brandeis, diventato intanto giudice supremo, nella sua celebre *dissenting opinion* nella causa *Olmstead Vs. United States* del 1928[23]. Si trattò del primo caso nella storia della Corte Suprema degli Stati Uniti di intercettazioni telefoniche[24], imperniato sulla presunta violazione, da parte degli agenti FBI, del Quarto Emendamento nei confronti di Roy Olmstead. Egli riteneva illegale la perquisizione nei suoi confronti dal momento che violava il Quarto Emendamento in quanto non gli era stata garantita una *"ragionevole aspettativa di privacy"*. Tuttavia, a fronte di una interpretazione letterale dell'emendamento in questione, si dava ragione alla posizione degli agenti federali, in quanto i cavi telefonici non appartenevano né all'ufficio né all'abitazione dell'imputato e dunque non erano di sua proprietà, il che significava che non poteva rinvenirsi una invasione fisica che avrebbe portato alla violazione del domicilio anche in assenza di mandato[25]. Nonostante il processo ebbe esito negativo per Olmstead, fondamentale fu, per l'appunto, la *dissenting opinion* del giudice supremo Brandeis.

---

[22] *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

[23] Olmstead vs. United States, U.S. Supreme Court, 277 U.S. 438, 1928.

[24] Nel caso di specie, Roy Olmstead aveva organizzato una attività illegale organizzata di contrabbando di alcol (in quello stesso periodo fu emanato un atto che proibiva la vendita, il consumo e la distribuzione di bevande alcoliche). L'attività era ben sviluppata anche grazie alle numerose linee telefoniche che permettevano il coordinamento fra i vari complici. Le prove raccolte per la sua imputazione furono ottenute proprio con intercettazione telefoniche predisposte dagli agenti dell'FBI ma senza la richiesta di un mandato per effettuare le stesse in quanto non era avvenuta alcuna violazione fisica di uffici o abitazioni personali.

[25] Sempre con una interpretazione discutibile, la Corte disse: "ritenere le linee telefoniche parte del domicilio sarebbe stato come ritenere tali anche le strade attraverso le quali esse si allungavano."

Infatti, così come quasi quarant'anni prima, al contrario dell'amico Warren, egli ribadisce quanto alcuni concetti giuridici debbano fare i conti col tempo e con l'evoluzione della società, in modo da evolversi di pari passo. Non a caso, ad apertura del suo discorso richiamò una celebre posizione del Chief Justice Marshall[26], con la quale volle evidenziare che una interpretazione così restrittiva del Quarto Emendamento mal si sposava con la necessità di far i conti con l'evoluzione tecnologica e scientifica del XX secolo; il tempo comporta cambiamenti imprevedibili che solo in una corretta interpretazione della volontà dei Padri Fondatori possono trovare una collocazione adeguata.

Egli continua sottolineando come siano ormai accessibili al governo molti espedienti subdoli ed invasivi della privacy, e che di certo non erano stati previsti dai creatori della Costituzione, fin quando ci si attenga ad una interpretazione strettamente letteraria. Conclude infine ponendo un quesito ancora più avanzato: *"Un giorno saranno trovati mezzi grazie ai quali il governo senza rimuovere alcuno scritto da cassetti segreti, potrà riprodurlo in tribunale e con cui gli sarà possibile esporre gli eventi più intimi che possono avvenire in una casa. Può essere che la Costituzione non garantisca alcuna protezione contro una tale invasione della sicurezza dell'individuo?"*.

Come è evidente, Brandeis cercava di enucleare dal caso di specie un problema ben più grave, che era quello di riconoscere come non ci si poteva affidare ad una semplice interpretazione letterale degli Emendamenti; per questo motivo egli esorta la Corte Suprema, come maggiore interprete costituzionale, a non fermarsi alle contingenze di uno stato tecnologico sempre in divenire e a tener conto del vero scopo dei Costituenti, ovvero, nel caso di specie, quello di proteggere il diritto ad essere lasciati soli.

Certamente possiamo rinvenire come la posizione del giudice Brandeis abbia fornito un assetto completamente nuovo e rivoluzionario sul problema che

[26] Vero e proprio baluardo del costituzionalismo americano, in *McCulloch vs. Maryland, 1819,* disse *"la nostra è una costituzione destinata a durare per i tempi a venire, e, di conseguenza, ad essere adattata alle varie problematiche degli affari degli uomini"*.

stiamo trattando, eppure, come anticipato, non furono sufficienti per essere accolte dalla Corte.

La prima affermazione giurisprudenziale del diritto alla privacy: il caso Katz vs. U.S.

Il ribaltamento totale avvenne, anche qui, quarant'anni dopo, nel caso che per eccellenza sancisce il primo accoglimento giurisprudenziale del diritto alla privacy da parte della Corte Suprema Americana: il caso *Katz vs. United States,* del 1967[27]. La questione fu sempre relativa ad un'intercettazione telefonica operata senza mandato[28] e che si ritenne violare il Quarto Emendamento. Dalla parte dell'accusa, si riteneva che nonostante l'emendamento garantisse una tutela contro le perquisizioni e le ricerche in assenza di mandato, non vi fosse nessun bene tangibile che fosse stato perquisito o ricercato, e dunque il Quarto Emendamento non poteva essere applicato, poiché la cabina telefonica era di proprietà pubblica e non costituiva quindi un'area costituzionalmente protetta. La difesa, d'altro canto, non poté non richiamare la vecchia *dissenting opinion* in *Olmstead. Vs. U.S.* dell'ormai defunto giudice Brandeis, che, questa volta, risultò decisiva tanto da essere accolta col voto favorevole di ben sette giudici ed uno solo contrario.

Interessanti le posizioni di alcuni giudici favorevoli, quali Potter Stewart e John Harlan, che ritengono come *"quello a cui Katz cercava di sottrarsi non era certo l'occhio indiscreto, ma semmai l'orecchio senza invito"*, intendendo come fosse necessario infondere un nuovo spirito interpretativo nel Quarto Emendamento il quale *"protegge le persone e non i luoghi"*. Proseguono sostenendo che se la polizia federale avesse richiesto un'autorizzazione del giudice prima di procedere o avesse avuto mandato, non ci sarebbe stata alcuna violazione nei confronti dell'imputato, mentre nel caso contrario, ovunque un individuo possa trovarsi, egli ha diritto di sapere che rimarrà

[27] Charles Katz vs. U.S., 389 US 347, 1967.

[28] Nel caso di specie, Katz era sospettato coinvolto in una attività di gioco d'azzardo a Los Angeles. Tenuto sott'occhio dalla polizia federale, si era notato che faceva spesso uso di una singola cabina telefonica che si ritenne fosse usata per trafficare informazioni derivanti da bische e allibratori. In assenza di mandato, ma senza entrare fisicamente nella cabina, gli agenti introdussero una cimice, posta all'esterno del telefono pubblico. In questo modo vennero registrate diverse conversazioni che permisero di chiedere la condanna di Katz in violazione di una legge federale che vietava il traffico di informazioni illegali sulle scommesse.

immune da ricerche e perquisizioni irragionevoli. Infine, nella sua *concurring opinion*, il giudice Harlan propone un significativo test a due fasi per riconoscere cosa fosse "privato" per il Quarto Emendamento e che, decisamente, pose le basi per la soluzione di diversi problemi che si sarebbero sviluppati negli anni a seguire in tema di diritto alla privacy: "*Bisogna chiedersi se esiste un duplice requisito, il primo dei quali è stabilire se la persona ha mostrato un'effettiva e soggettiva aspettativa di privacy, mentre il secondo è che quell'aspettativa sia riconosciuta dalla società come ragionevole*"[29], nel caso in cui entrambe le aspettative siano soddisfatte, potrà ritenersi tale diritto alla privacy protetto dal Quarto Emendamento[30]. La decisione della Corte nel caso ora analizzato, ed il test proposto dal giudice Harlan, sicuramente hanno fornito un fondamentale balzo concettuale iniziando un percorso progressivo di tutela che, fino a quel momento, era vivo soltanto fra le pagine dottrinali degli studiosi di diritto e che mai aveva ancora avuto un appoggio sostanzioso sul fronte giurisprudenziale. Di certo, a fronte della proposta del giudice Harlan, che pian piano fu immagazzinata nei meccanismi della Corte Suprema[31], il Quarto Emendamento, in tema di diritto alla privacy, assunse connotati certamente più moderni; esso infatti a fronte di questa nuova luce, diede vita alla necessità di compiere accurate scelte di valori, come un equo bilanciamento tra gli interessi in contrasto, dando anche un significato sostanziale a espressioni quali "ragionevole aspettativa di

Le conseguenze del test proposto dal giudice Harlan

[29] Charles Katz vs. U.S., 389 US 347, 1967.

[30] Per un'analisi più approfondita del test proposto dal giudice Harlan e delle sue conseguenze nella giurisprudenza della Corte Suprema si veda *A reconsideration of the Katz Expectation of Privacy Test, in* 76 *Michigan Law Review,* University of Michigan, 1977.

[31] L'accoglimento di tale posizione tuttavia non fu unitaria; si veda, ad esempio, *New York vs. Burger, 482 U.S. 691, 1987:* in questo processo, la Corte stabilì un principio per cui ove è già presente una stretta regolamentazione di una determinata attività, l'aspettativa di privacy costituzionale diminuisce in corrispondenza. In questo senso, analizzando le oscillazioni della Corte in tema di Quarto Emendamento successivo al caso *Kratz,* è rinvenibile la posizione di Thomas Clancy in *Thomas K. Clancy, What does the Fourth Amendament Protect? Proprety, Privacy or Security?,* in *Wake Forest Law Review,* vol. 33, 1998 pp. 344 e ss.. L'Autore riconosce come la Corte Suprema, mentre prima del caso *Kratz* avesse come oggetto di protezione del Quarto Emendamento un assetto proprietario, nel periodo successivo abbia avuto spesso posizioni altalenanti dovute ad una composizione più o meno liberale della Corte stessa.

privacy" e all'aggettivo "ragionevole" riferito alle perquisizioni e confische da parte degli enti governativi.

Non è un caso, infatti, se, a fronte della posizione del giudice Harlan, si siano sviluppate tutta una serie di situazioni particolari quali la cd. "esposizione volontaria" [32], vale a dire casi individuabili come eccezioni al Quarto Emendamento inteso circa il diritto alla privacy che dunque permetterebbero ad esempio un'ispezione anche senza mandato. Ne possiamo individuare almeno tre, che, ovviamente, non sono altro che concetti embrionali che poi, in seguito, troveremo nuovamente nell'analisi della nostra normativa nazionale arricchiti da un ulteriore evoluzione socio-giuridica.

Uno è il caso in cui una persona consenta ad esempio l'accesso alle informazioni che la riguardano rendendo in questo modo superfluo il mandato specifico[33]; è evidente come questa situazione non sia altro che una specie di pre-evoluzione del più ampio concetto dell'informativa privacy e della necessità del consenso.

Una seconda vicenda potrebbe essere quella in cui un individuo riveli delle informazioni ad un terzo[34]. In questo caso, al momento della rivelazione, magari compromettente, egli si assume il rischio che il terzo possa rivelarla alle forze dell'ordine. Con le dovute precauzioni di una simile proporzione, tale questione è assimilabile alla cd. "comunicazione volontaria", ricavabile in via interpretativa dall'art. 25 del Codice della Privacy, rubricato "divieti di comunicazione e diffusione".

---

[32] Termine usato anch'esso da Thomas Clancy che, nel medesimo articolo, ritiene come *"un approccio normativo e liberale sia particolarmente necessario nel mondo odierno, dove la tecnologia minaccia di rendere tutti i dettagli della vita di una persona rilevabili"* e dunque alla luce della evoluzione tecnologica bisogna ricostruire in modo attuale il significato di esposizione volontaria.

[33] Uno dei primi casi, sempre negli Stati Uniti, fu *U.S. Supreme Court, Scneckloth vs. Bustamonte, 412 U.S. 218,219, 1973*

[34] Fu il caso che si sviluppò in U.S. Supreme Court, *United States vs. Miller, 425 US 435, 442-43, 1976,* ove la Corte dovette decidere se si trattasse di ragionevole aspettativa privacy sul segreto bancario la situazione in cui un titolare di un conto corrente ritenesse di non volere che fossero conosciute le sue informazioni e dati bancari da dipendenti diversi da quelli della banca con la quale fosse vincolato. La Corte ribaltò totalmente la questione, in quanto ritenne che non v'era alcuna ragionevole aspettativa privacy da parte sua, dal momento che il contenuto degli assegni non fosse equiparabile ad informazioni confidenziali, bensì uno strumento commerciale volontariamente trasmesso all'istituto di credito.

L'ultimo caso è quello in cui un'informazione sia chiaramente visibile al pubblico e quindi aspettarsi che quest'informazione rimanga privata non potrebbe definirsi ragionevole [35]. Il parallelismo è rintracciabile con l'informazione pubblica utilizzabile per finalità e scopi correlati al fatto del dato reso pubblico, come espresso ad esempio nell'allegato A1, sempre del Codice della Privacy, relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica.

Le posizioni dottrinali che si sviluppano assieme all'evoluzione della Corte

È evidente come questi esempi pongano modalità diverse di esposizione volontaria dell'individuo che sono state ritenute non rientranti nella protezione del Quarto Emendamento relativamente al diritto alla privacy nel momento in cui, controbilanciate con un diverso interesse costituzionale, siano state ritenute di rango inferiore e quindi sacrificabili. In opposizione a queste posizioni, forse dovute anche alla mancanza, fino ad allora, di una normativa definita, diversi Autori [36], tentando di fornire il loro contributo alla causa, ritennero che, ancora una volta, le interpretazioni della Corte sul Quarto Emendamento erano state troppo restrittive e passive nei confronti della evoluzione tecnologica, dal momento che in fin troppe situazioni le garanzie costituzionali in tema privacy erano state scavalcate da altrettanti interessi e situazioni che, nonostante fossero contingenti, avevano prevalso.

In un certo senso, sebbene dal caso *Katz* si fosse registrata una netta evoluzione in tema privacy, dal momento che ci si sganciò completamente dal

[35] Trattasi del caso avutosi in *U.S. Supreme Court, Horton vs. California,* 496 US 128, 133 & N.5, 1990 ove l'informazione era visibile pienamente da parte delle forze dell'ordine. Esse avevano un regolare mandato per la perquisizione di un abitazione al fine di ricercare alcuni gioielli rubati, durante la ricerca, sono travate armi illegali in piena vista; la Corte ritenne non rientrante la situazione nel Quarto Emendamento dato che le armi erano facilmente visibili da chiunque entrasse nell'appartamento.

[36] Senza pretese di completezza, dagli esempi che seguono si può notare come l'apporto dottrinale sia stato un indubbio appoggio, assieme all'operato della Corte, per l'evoluzione del diritto alla privacy: uno di questi fu William Prosser che in W.L. Prosser, *Privacy, a legal analysis,* in *California Law Review,* n.48, 1960, pp. 383-423, in uno studio sugli illeciti civili fondato su oltre trecento casi, afferma che il diritto alla privacy abbracci più tipi di lesioni corrispondenti a più interessi della persona, come l'appropriarsi del nome altrui, l'irragionevole intrusione nella sfera privata di un terzo, ecc. Il suo elaborato fu fonte di ispirazione per molti stati federali che trasformarono in "*Torts*" gli illeciti da lui rintracciati, e che dunque vennero legalmente riconosciuti.

taglio prettamente proprietario fornito al Quarto Emendamento, per approdare al riconoscimento di un diritto alla privacy, accompagnato dalla dotta posizione del giudice Harlan, si ritenne come in effetti la Corte Suprema non avesse sufficientemente recepito tale evoluzione, dal momento che, in alcune sue pronunce, aveva lasciato prevalere a discapito del diritto alla privacy, altri interessi che, come detto, avevano un valore solo contingente.

Forse però, una posizione così critica nei confronti dell'operato della Corte Suprema non è del tutto condivisibile. L'apporto di essa al tema del diritto alla privacy, successivamente al caso *Kratz,* accompagnata anche dalle coadiuvanti posizioni dottrinali[37] sviluppatesi in tal senso, non può negarsi, seppur con qualche riserva, poiché, senza dubbio, senza di esso non si sarebbero originate le iniziali normative americane in tema di riservatezza[38] che, tutt'oggi, nelle loro forme successive, continuano, in connubio all'operato della Unione Europea a mandare segnali evolutivi al nostro continente. Inoltre, da ultimo, non si può dimenticare come, grazie all'apporto della Corte, il diritto alla privacy abbia aggiunto alla sua originale caratteristica negativa (*Right to be let alone*), una successiva caratteristica positiva, intesa come il diritto della persona di attivarsi al fine di controllare tutte le informazioni che la riguardano e che queste vengano trattate da terzi solo in caso di necessità.

[37] Interessante, in tal senso, è la posizione di Edward Bloustein, che si sviluppa in senso critico rispetto all'approccio di Prosser, aggiungendo un ulteriore tassello al quadro dottrinale che si è delineato a supporto della giurisprudenza: BLOUSTEIN E., *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, in *New York University Law Review*, 39: 962–1007, 1964. La critica principale poggia sulla visione pluralistica del Prosser alla quale Bloustein contrappone una visione unitaria della privacy, inteso come concetto che esprime un valore essenziale all'uomo e che si ripercuote in tutti gli ambiti normativi cui si riferisce. Riprende la posizione del giudice Brandeis asserendo, come principio generale che sottace a quello della privacy, il principio di una personalità inviolabile per cui la privacy diventa un concetto essenziale per il raggiungimento della felicità, uno dei valori primari della costituzione statunitense.

[38] Non è questo il tema centrale della trattazione ma, per completezza informativa, si ricordano il *FOIA, Freedom of Information Act* del 1966, che assicura al cittadino l'accesso a tutte le informazioni sugli enti pubblici tramite un determinato metodo di pubblicità; il *Privacy Act del 1974* che integrando il FOIA pone una barriera alla circolazione delle informazioni che riguardano il cittadino ed agevola il "diritto di sapere" da parte degli investigati.

4. Il riconoscimento del diritto alla privacy all'interno dei diritti della personalità in Europa

Sebbene la ricerca e l'evoluzione di un diritto alla privacy all'interno del nuovo continente sia stata certamente tortuosa ed impegnativa, per i motivi che abbiamo trattato fino ad ora, di certo l'esperienza nel nostro continente non può essere da meno. Se negli Stati Uniti un appoggio forte è stato fornito dalla Corte Suprema che, in conclusione, ha tenuto fede alle premesse da cui era partita, in Europa tale elemento unificatore è mancato. Infatti, la tradizione romanistica dei sistemi giuridici europei, ognuno con le proprie differenze, è stata la principale ragione di una grande difficoltà ad ostacolo del raggiungimento di un accordo sul diritto in questione: nonostante sarà in buona parte l'Italia a far ordine in tema di origini sul concetto di riservatezza all'interno dei diritti della personalità, in un primo momento, a cavallo fra il XVIII ed il XIX secolo, un primo accenno storico-giuridico può essere trovato in area germanica.

L'esperienza germanica

Fu infatti in quel periodo che, per la prima volta, si sviluppa la discussione sull'esistenza di una categoria di diritti nota come *"Persönlichkeitsrechte"*[39] o anche detta *"Individualrecthe"*[40]. Tale concezione si originava dalla tradizione della filosofia giuridica tedesca che riconosceva nel Diritto Naturale la fonte primaria di ogni principio legale. Di tali *"Individualrecthe"* si riconosceva una definizione piuttosto ampia, intendendoli come quella cerchia di diritti della personalità sulla quale l'individuo esercita una posizione di signoria. Tuttavia, proprio perché ci si muoveva ancora su un campo più filosofico che giuridico, tutti questi svariati diritti avevano in realtà ben poco in comune fra di loro, tant'è che parte di questi non ebbero nemmeno un riconoscimento

[39] La paternità di questa posizione è attribuita a GIERKE O., *Deursches Privatrecht*, I, Lipsia, 702 e ss., come riportato da ZENO-ZENCOVICH, V., *"Personalità (diritti della)"*, in "Digesto delle discipline penalistiche", 1995.
[40] Si tratta dei "diritti della personalità" e dei "diritti dell'individuo".

nell'ordinamento positivo. Tra questi, quelli che più di tutti vennero riconosciuti furono certamente i diritti all'onore e al nome.

Il vero problema, in realtà, era che alla filosofia del diritto naturale si opponeva il periodo storico del positivismo legale, con la conseguenza, come detto, di non veder riconosciuti la maggior parte di questi diritti. Infatti, all'interno del *Bürgerliches Gesetzbuch*[41] al §823 1° comma, ove sono presenti i beni giuridici la cui lesione consente l'azione di risarcimento del danno, non è del tutto presa in considerazione l'eventualità della lesione di beni come l'onore e l'intimità della sfera privata[42].

Una forte opera motivazionista su questo tema venne principalmente da parte di tre autori, Gareis, Gierke e Kohler, che cercando di suscitare un nuovo interesse sul tema dei diritti della personalità, contribuirono alla prima legittimazione della protezione di questi diritti in Svizzera[43]. Il primo di questi ritiene che esistano diversi diritti della personalità, aventi tutti la medesima rilevanza, mentre per Gierke e Kohler esiste un singolo e generico diritto della personalità di cui gli altri presunti diritti in realtà altro non sono se non indirette espressioni. Aggiunge Kohler infine, con un chiaro riferimento ad un aspetto del diritto alla riservatezza, che fra questi vi è un "diritto alla segretezza" che protegge l'individuo dalla pubblicazione indesiderata di rapporti epistolari e dalla rivelazione di fatti della vita privata[44].

L'esperienza francese

Questo dibattito sul riconoscimento giuridico dei diritti della personalità raggiunge rapidamente anche gli stati confinanti, fra cui la Francia. Uno dei primi e più importanti riferimenti dottrinali che si ricordano fu quello di

[41] Abbreviato con BGB, è il codice civile tedesco, che entrò in vigore il 1 gennaio del 1900. Il suo sviluppo comincia nel 1881, in pieno II Reich. Ciò significa, come accennato, che la forte spinta positiva proveniente da quel tipo di forma di stato fu probabilmente la causa principale che giustifico la mancata presenza all'interno del codice di quegli influssi derivanti dalla filosofia giuridica del diritto naturale.

[42] Questa posizione è rinvenibile in ZWEIGERT-KOTZ, *Introduzione al Diritto Comparato,* volume secondo, Milano 1995, pp. 299 e ss.

[43] All'art. 28 del *Zivil Gedetzbuch* svizzero del 1912 è detto che: "chiunque sia stato leso nei suoi rapporti personali da un'altra persona può richiedere la cessazione delle turbative e, qualora, l'altro abbia agito colposamente, ha diritto al risarcimento dei danni". In questo modo si è demandato al giudice la decisione su cosa si debba intendere per lesione dei rapporti personali, potendo tutelare in questo modo sia l'onore che l'intimità degli individui.

[44] KOHLER G., *Das Autorrecht,* in *Iherings Jahrbucher,* XVII, 1880.

Alphonse Boistel[45], anch'egli giusnaturalista, che basandosi principalmente sul diritto d'autore, sviluppa la nozione di *droit moral,* che rapidamente acquista anche una collocazione nel sistema giuridico francese. Infatti nel 1909 nasce la categoria dei diritti della personalità, supportata anche da un altro giurista francese, Perreau[46], il quale sviluppa la sua posizione basandosi sulla norma di chiusura del *Code civil* all'articolo 1382[47]. A fronte non di una tutela diretta, ma in ragione di una norma aperta come quella ora citata, l'Autore rintraccia e giustifica la necessità della *protection de la vie privèe*[48] per cui, a fronte di un pregiudizio o di un danno ingiusto, il giudice dovrà comminare una sanzione risarcitoria.

È tuttavia evidente come, a fronte dei cenni ora riportati, si è ancora piuttosto lontani da una sufficiente tutela dei diritti della personalità e, di conseguenza, di un diritto alla riservatezza. Di fatti, come vedremo a breve, e come è stato accennato in precedenza, il passo successivo avviene proprio in Italia, per mano di Adolfo Ravà, docente di filosofia del diritto, il quale, partendo da un'analisi del "*Tractatus de potestate in seipsum"* di Baldassarre de Amescua, giurista spagnolo del XVI secolo, compie un interessante analisi fra filosofia e diritto per individuare la personalità dal punto di vista giuidico intesa come "diritto sulla propria persona"[49].

[45] BOISTEL A., *Cours de philosophie du dreoit,* Parigi, 1899.
[46] PERREAU V., *Les droits de la personnalite, in Rev. Trim. d. Civ.,* Parigi, 1909.
[47] "Ogni atto commesso da un uomo danneggiando un altro, obbliga chi ha causato il danno a risarcire."
[48] "Protezione della vita privata".
[49] RAVA' A., *I diritti sulla propria persona nelle scienza e nella filosofia del diritto,* Torino, 1901.

5. *Le posizioni della dottrina e della giurisprudenza italiana prima delle leggi sulla privacy: il bene giuridico nella Costituzione*

Dai diritti della personalità al diritto alla riservatezza: la posizione di Ravà

Gli studi filosofico-giuridici, compiuti da Alfonso Ravà agli inizi del XX secolo, furono uno dei motori che, negli anni a venire, giustificarono il forte dibattito che si venne a creare attorno ai diritti della personalità e, nello specifico, attorno al diritto alla riservatezza, dal momento che, col passare del tempo, nacquero i primi indizi normativi che, sotto la corretta angolazione, lasciavano trapelare seppur in via indiretta alcuni aspetti di questi diritti.

Siccome era ancora assente un esplicito riconoscimento di un autonomo diritto alla riservatezza nell'ordinamento, la sua giustificazione venne rinvenuta facendo leva su quelle norme che ne erano, in qualche maniera, una manifestazione. Ravà intuì che *"la qualità di persona richiede ed esige che alla persona stessa sia riservata una certa sfera relativa ai dati più gelosi e più intimi di essa e della sua attività"*[50], da ciò, secondo lui, scaturisce un generale diritto alla riservatezza dalle molteplici implicazioni. A giustificazione di ciò, l'Autore richiama norme quali l'art. 10[51] del Codice Civile del 1942 e soprattutto gli art. 96 e 97[52] della legge sul Diritto d'Autore del 22 aprile 1941. In virtù di un procedimento analogico, il diritto alla riservatezza si ricava in quanto avente *eadem ratio* delle norme citate, nella parte relativa all'immagine. Alla base della tesi dell'Autore, soggiace, come

[50] RAVA' A., *Istituzioni di diritto privato,* Cedam, Padova, 1938, pp.174-175.

[51] "Qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dai casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni".

[52] Art. 96: "Il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa, salve le disposizioni dell'articolo seguente". Art. 97 : "Non occorre il consenso della persona ritrattata quando la riproduzione dell'immagine è giustificata dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici o didattici o culturali, o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico. […] Il ritratto non può tuttavia essere esposto o messo in commercio, quando l'esposizione o messa in commercio rechi pregiudizio all'onore, alla reputazione od anche al decoro della persona ritratta".

riferimento, l'art. 12 2° comma[53] delle disposizioni sulla legge in generale. Com'è noto, l'articolo, oltre al caso di *analogia legis* citato, contempla anche la cd. *analogia iuris,* vale a dire quell'interpretazione costituita dal ricorso ai principi generali dell'ordinamento giuridico dello Stato. In questo modo Ravà sottolinea la rilevanza assoluta degli attributi fondamentali della personalità umana come presupposto della libera esplicazione della persona stessa, così da affermare l'indubbia considerazione di essi da parte dell'ordinamento giuridico al di là di ogni espressa manifestazione di volontà del legislatore. Come conseguenza di questo ragionamento, l'Autore conclude rinvenendo nel novero dei diritti della personalità anche il diritto alla riservatezza, rintracciando in questo modo l' esistenza di un principio generale a tutela della stessa.

Critiche dottrinali: il diritto o i diritti della personalità?

Su una posizione completamente opposta si pone la dottrina del Pugliese[54], il quale ritiene come, in realtà, queste norme siano poste a protezione di un bene superiore al singolo individuo, vale a dire la personalità stessa della persona. Con forti influenze di diritto positivo[55], egli afferma che non esiste alcuna norma che riconosca espressamente il diritto alla riservatezza e che nemmeno si può raggiungere con l'estensione analogica, in quanto, le norme richiamate dal Ravà sarebbero norme che, ai sensi dell'art. 14[56] delle disposizioni sulla legge in generale, farebbero eccezione alle regole generali per le quali vige il divieto di analogia.

Oltre al dibattito sull'esistenza dei diritti della personalità, si instaura un ulteriore dibattito sulla loro eventuale unicità o molteplicità. Giampiccolo[57], ricalcando le orme tedesche di Gierke, e sostenuto da alcune posizioni della

[53] "Se una controversia non può essere decisa con una precisa disposizione, si ha riguardo alle disposizioni che regolano casi simili o materie analoghe; se il caso rimane ancora dubbio, si decide secondo i principi generali dell'ordinamento giuridico dello Stato".

[54] PUGLIESE G., *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche,* Foro It., Zanichelli, Bologna 1954, parte I., pp.118-120.

[55] È impossibile non notare come una posizione di questo tipo sia figlia del periodo storico in questione, per il quale anche i diritti personalissimi dell'individuo appartenevano allo Stato.

[56] "Le leggi penali e quelle che fanno eccezione a regole generali o ad altre leggi non si applicano oltre i casi e i tempi in esse considerati".

[57] GIAMPICCOLO G., *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza,* in Riv. Trim. dir. Proc. Civ., 1958, p. 465 e ss.

giurisprudenza costituzionale, delinea un unico diritto della personalità, secondo la posizione monista, considerando la persona umana come valore unitario e traendone come logica conseguenza che il complesso di norme presenti nell'ordinamento non costituiscono il fondamento di tanti autonomi diritti della persona bensì piuttosto la disciplina specifica di alcuni aspetti particolari della sua tutela, ipotizzando dunque un rapporto di genere a specie fra diritto unitario e singole disposizioni. Nonostante i vantaggi di questa posizione, che garantisce maggiore elasticità e adattamento alle norme, essa non fu esente da critiche[58]. Su tutti infatti si ricorda De Cupis che, in un suo trattato[59], supporta invece la posizione pluralista dei diritti della personalità, giustificata dalla molteplicità di singoli e specifici aspetti e interessi della persona (il nome, l'immagine, la reputazione, ecc), ognuno con caratteristiche peculiari e dotate di propria autonomia. Tuttavia, per il momento, questo tipo di problema permane in secondo piano, poiché l'evoluzione dottrinaria in tema di diritto alla riservatezza ha sempre dovuto fare i conti con l'evoluzione giurisprudenziale della Corte di Cassazione sul tema che, nei primi momenti, tardava a fornire appoggi certi.

Le prime sentenze in tema di riservatezza

I primi casi, negli anni '50, provenivano da una giurisprudenza di merito che affrontò diversi casi sviluppatisi da opere cinematografiche e pubblicazioni relative a vicende personali di personaggi noti. Tra questi per primo se ne ricorda uno[60], in ambito cinematografico che, una volta giunto in Cassazione[61], diede esito negativo circa il diritto alla riservatezza. Infatti secondo la Corte *"nessuna disposizione di legge autorizza a ritenere sancito come principio generale il rispetto assoluto dell'intimità della vita privata salvo che l'operato dell'agente, offendendo, ricada nello schema generale del fatto illecito".*

[58] Si veda, nuovamente, ZENO-ZENCOVICH, V., *"Personalità (diritti della)"*, in "Digesto delle discipline penalistiche", 1995.
[59] DE CUPIS A., *I diritti della personalità,* in Tratt. Di diritto civile e commerciale, Giuffrè editore, Milano, 1982, IV, p. 271.
[60] Si trattava di un film sul tenore Enrico Caruso, "Leggenda di una voce", circa il quale i familiari del defunto cantante chiesero l'inibitoria del film poiché lesivo della riservatezza del loro congiunto.
[61] Corte di Cassazione, ss. 22 dicembre 1956, n. 4487, in Giur. Ut., 1957, I, p. 366.

Dunque, secondo il generale principio del *neminem laedere* dell'art. 2043 del Codice Civile, il tema poteva trovare ivi soluzione, senza la necessità di sviluppare nuovi istituti. Sebbene ora tale sentenza possa apparirci ai limiti dei nostri principi giuridici, tuttavia, nel lontano 1956, vantava diverse giustificazioni. Una su tutte è quella per cui, in virtù di una Costituzione senza dubbio nuova, mancava ancora nella quotidiana attività giurisprudenziale, una preponderante attività interpretativa sulla stessa che avrebbe, nel tempo, garantito delle letture più aperte dei principi cardine dell'ordinamento[62]. L'articolo fondamentale su cui si incentra la maggior parte del bene giuridico riservatezza, e sul quale sin da quel momento si sarebbe dovuto partire, (che invece allora non fu preso in considerazione) era l'art. 2 della Costituzione[63]. La situazione, invece, mutò fortemente con la sentenza n. 990 del 1963 della Corte di Cassazione[64], la quale si occupò di un caso particolarmente discusso dall'opinione pubblica di quei tempi[65] e che, per questi motivi, diede vita ad una sentenza decisiva. Nella massima si legge *"Sebbene non sia ammissibile il diritto tipico alla riservatezza, viola il diritto assoluto di personalità, inteso quale diritto erga omnes alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo, la divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito, ed ove non sussista, per la natura dell'attività svolta dalla persona e del fatto divulgato, un preminente interesse pubblico di conoscenza"*.

Com'è chiaro, nonostante ancora manchi un diritto tipico alla riservatezza, viene riconosciuto un diritto unitario assoluto della personalità, secondo la posizione monista precedentemente accennata; ciò fu decisamente il primo

[62] Ed ecco che torna attuale il paragone che si fa con l'attività interpretativa americana che si propose in tema di IV Emendamento e che fu il punto di svolta per la nascita del diritto alla privacy.

[63] " La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale."

[64] Cassaz. Civ., sentenza n.990 del 20 aprile 1963, in Foro it., Zanichelli, Bologna, I, 1963, p.877 commentata da A. De Cupis.

[65] Il settimanale "Tempo" aveva pubblicato una serie di articoli con alcuni particolari sulla vita intima di Claretta Petacci, amante del Duce; i suoi congiunti fecero causa al settimanale in quanto esso aveva anche divulgato dettagli e descrizioni ritenute offensive da parte degli stessi congiunti.

vero passo che costituì il diritto del quale ci accingiamo a studiare. Tuttavia, per come venne strutturato, il risultato fu, per la dottrina, insoddisfacente. Coloro i quali auspicavano che venisse sancito tipicamente il diritto alla riservatezza rimasero insoddisfatti, in quanto l'indirizzo della Corte era troppo povero per dare un preciso riconoscimento sostanziale ed autonomo ad esso, mentre chi negava un fondamento giuridico al diritto, rinveniva come, tuttavia, la posizione della Corte fosse diventata sin troppo favorevole (rispetto alle precedenti) ad accogliere un alveo di diritti che, presto o tardi, avrebbe fatto germogliare il diritto in questione.

Il caso della svolta: la sentenza n. 2129 del 1975

La situazione permase in questo stato di incertezza fino al 1975, anno in cui si registrò la svolta definitiva, con un'ulteriore sentenza di Cassazione[66] che affermò definitivamente l'esistenza di un diritto alla riservatezza. A seguito dell'analisi del caso di specie[67], la Corte rilevò un duplice fondamento, implicito ed esplicito, del diritto alla riservatezza. Il primo viene individuato *"in quel complesso di norme ordinarie e costituzionali che, tutelando aspetti peculiari della persona, nel sistema dell'ordinamento sostanziale, non possono non riferirsi anche alla sfera privata di essa[68]"*, mentre il secondo *"in tutte quelle norme, contenute in modo particolare in leggi speciali, nelle quali si richiama espressamente la vita privata del soggetto o addirittura la riservatezza[69]"*. Ecco che, probabilmente con un ritardo di quasi mezzo

[66] Cass. Civ., Sentenza del 27 maggio 1975, n. 2129.

[67] Come negli altri casi, l'episodio è relativo a personaggi di pubblico interesse: Sorāyā Esfandiyāri, seconda moglie di Mohammad Reza Pahlavi, ultimo Scià di Persia, era stata fotografata in compagnia di un uomo in atteggiamenti intimi all'interno della sua abitazione, e queste foto erano state pubblicate da alcune delle principali testate giornalistiche nazionali contro le quali la donna intentò causa.

[68] La Corte ne cita alcuni quali: diritto al corpo (art. 5 c.c.), al nome (artt. 6-9 c.c.), all'immagine (art. 10 c.c.), all'anonimato e all'inedito (artt. 21 e 24 legge dir. d'Autore), all'onore contro la rivelazione di fatti determinati (art. 595, secondo comma, c.p.) al domicilio (art. 614 c.p.), alla corrispondenza (artt. 616 c.p. e 48 legge fall.).

[69] Riguardo alle notizie raccolte in sede di rilevazioni statistiche (art. 19 r.d.l. 27 maggio 1929, n. 1285); facendo divieto di pubblicare corrispondenza o memorie che « abbiano carattere confidenziale o si riferiscano alla intimità della vita privata » (art. 93 legge n. 633/1941); con l'obbligo dei lavoratore domestico di « mantenere la necessaria riservatezza per tutto quanto si riferisca alla vita familiare » (art. 6 legge n. 339/1958); si è perfino derogato al principio della pubblicità del dibattimento penale « quando la lettura o l'ascolto possono ledere il 'diritto alla riservatezza' di soggetti estranei alla causa ovvero, relativamente a fatti estranei al processo, il diritto delle parti private alla riservatezza » (art. 7 legge n. 98/1974).

secolo, la Corte si decide a sviluppare in maniera definitiva l'articolo 2 della Costituzione, alla luce del diritto in questione. Essa infatti, riprendendo la sua antecedente posizione[70], che rinveniva nell'articolo la presenza di un diritto assoluto unitario della personalità, aggiunge che, nell'alveo di questo diritto, è presente anche il diritto alla riservatezza. Infatti, dal momento che la Repubblica garantisce i diritti inviolabili dell'uomo nei quali è assolutamente imprescindibile quello della personalità, allo stesso modo lo è il diritto alla riservatezza, definito dalla Corte come *"il diritto che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari, le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione e il decoro, non siano giustificate da interessi pubblici preminenti*"[71].

Tuttavia, per giungere ad una definizione di questo tipo, la Corte dovette compiere necessariamente un rapido *excursus* sulle posizioni sino a quel momento rintracciabili sul tema, facendo anche chiarezza dal punto di vista lessicale. Viene infatti subito evidenziato che con l'espressione «diritto alla riservatezza», una delle prime e più usate formulazioni del fenomeno, sono indicate diverse ipotesi, che implicano un problema, non solo formale, ma anche sostanziale, e che si possono sintetizzare in tre aspetti.

La prima, che tende a restringere rigorosamente l'ambito di questo diritto nella concezione della "intimità domestica", si ricollega al concetto ed alla tutela del domicilio secondo il *"right to be let alone"* anglosassone.

Nella seconda, opposta, la Corte rintraccia formulazioni fin troppo generiche come "il riserbo della vita privata" da qualsiasi ingerenza, o la c.d. "privatezza" (privacy) cui corrisponderebbe un sostanziale ambito troppo vasto o indeterminato della sfera tutelabile.

[70] La sentenza Cass. Civ. n. 990 del 1963, sopra analizzata.
[71] Cass. Civ., Sentenza del 27 maggio 1975, n. 2129.

Come sopra riportato la Corte accoglie invece una posizione intermedia, la terza, che riporta in limiti ragionevoli la portata di questo diritto e che può identificarsi nelle formule che fanno riferimento ad una certa sfera della vita individuale e familiare, alla illesa intimità personale in certe manifestazioni della vita di relazione, a tutte quelle vicende, cioè, il cui carattere intimo è dato dal fatto che esse si svolgono in un domicilio ideale, non materialmente legato ai tradizionali rifugi della persona umana. È interessante notare come, in questo modo, la Corte fa convogliare i vari orientamenti dottrinari e giurisprudenziali precedenti, pervenendo ad una soluzione unica e solida per il futuro; inoltre, a supporto ulteriore del suo orientamento, la Corte richiama anche altri articoli della Costituzione [72] e vari spunti dal calibro internazionale [73] , che corroborano ulteriormente la sua posizione. Probabilmente la lunga attesa per tipizzare il diritto alla riservatezza si è rivelata necessaria; la Corte, prima di compiere un passo di questo tipo, ha atteso che vi fossero sufficienti appigli non solo nazionali, ma anche internazionali, senza dimenticare che, avendo la Costituzione ampiamente

[72] Sono richiamati l'art. 3 dal punto di vista dell'uguaglianza sostanziale, l'art. 13, circa l'inviolabilità della libertà personale, gli artt. 14 e 15, per l'inviolabilità di domicilio, della libertà e della corrispondenza, l'art. 27 dal quale dovrebbero trarsi dei limiti alla diffusione di notizie vicende dell'imputato e sui cd. « retroscena » dei delitti, l'art. 29 comma 2 che riconosce il carattere originario e l'inviolabile autonomia della famiglia e l'art. 41 laddove l'iniziativa economica trova un limite nel rispetto della libertà e della dignità umana.

[73] Si riportano le parole della Corte nella citata sentenza: "Giova appena accennare alla Dichiarazione universale sui diritti dell'uomo (approvata il 10 dicembre 1948 dall'ONU), ed al Patto internazionale relativo ai diritti civili e politici, approvato dall'Assemblea dell'ONU con risoluzione 16 dicembre 1966, n. 2200, dai quali risulta vietata qualsiasi interferenza arbitraria nella « vita privata » dell'individuo. Parimenti la Convenzione europea, firmata a Roma il 4 novembre 1950 (resa esecutiva con I. 4 agosto 1955, n. 848), ha ribadito che « toute personne a droit au respect de sa vie privée et familiare, de son domicile et de sa correspondence » (art. 8), stabilendo altresí che la libertà di pensiero trova un limite nella « protectioir de la réputation ou des droits d'autrui, pour empécher la divulgation d'informations confidentielles»(art. 10, n. 2).
Il contenuto di queste disposizioni è stato fatto proprio e sviluppato dalla risoluzione n. 428 del 1970 dell'Assemblea dei Consiglio d'Europa, che ha precisato *« le droit au respect de la vie privée ... doit proteger t'individui non seulement contre l'ingérence des pouvoirs publics, mais aussi contre celle des particuliers et des institutions privées, comprise les moyens de communication de masse ».*
La stessa Convenzione europea dei 1950 fornisce un preciso quadro dei limiti in cui il diritto alla riservatezza deve essere riconosciuto, stabilendo che l'ingerenza nella vita privata della persona può essere consentita quando essa sia *« prévue par la loi, et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nazionale, à la súreté publique, au bien-étre économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* »."

superato la maggiore età, si era ormai pervenuti ad una certa dimestichezza nella sua interpretazione che consentiva ormai di attualizzarla man mano che continuava a maturare, secondo la visionaria concezione dei Padri Costituenti. Tuttavia questa sentenza, ottima come punto di partenza, altro non è che l'inizio, la nascita di questo diritto. Essa sarà considerata come lo snodo fondamentale che, assieme ai successivi influssi comunitari, avrebbe giustificato le successive leggi in materia di riservatezza le quali, tutt'oggi, sono i solidi cardini sui quali poggia tutto il sistema che approfondisce il concetto di privacy e che, a breve, ci accingeremo ad analizzare.

6. La direttiva 95/46/CE e la L. 675/96

La normativa europea in tema di trattamento dei dati personali

Così come in Italia, anche nel resto d'Europa, la seconda metà del XX secolo fu fortemente caratterizzata da un evoluzione giuridica in tema di diritto alla riservatezza. Un primo vero provvedimento cogente europeo si rinviene nella Convenzione di Strasburgo del 28 gennaio 1981 n. 108[74] che approfondisce l'art. 8[75] della CEDU precedentemente accennata. Dal contenuto ancora embrionale, tale Convenzione sancisce all'art. 1 come suo scopo quello di garantire, sul territorio di ogni nazione aderente, ad ogni persona fisica, qualunque siano la sua cittadinanza o residenza, il rispetto dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata, nei confronti dell'elaborazione automatizzata dei dati di carattere personale che la riguardano (protezione dei dati).

Come si evince, nel diritto alla riservatezza comincia a prendere piede in modo sempre più preponderante la componente positiva rientrante nella cd. tutela e protezione dei dati personali, che ha la sua definitiva regolamentazione in modo ampiamente dettagliato nella direttiva 95/46/CE[76]. Essa si instaura su un concetto cardine che sarebbe stato alla base di ogni normativa nazionale, per il quale i sistemi di trattamento dei dati sono al servizio dell'uomo indipendentemente dalla sua nazionalità o residenza, e ne debbono rispettare le libertà e i diritti fondamentali, in particolare la vita privata. In questo modo la direttiva è stata costruita al fine di proteggere i diritti e le libertà delle persone in ordine al trattamento dei dati personali stabilendo i principi relativi alla legittimazione del trattamento dei dati.

---

[74] Recepita in Italia con la Legge 21 febbraio 1989, n. 98.

[75] Diritto al rispetto della vita privata e familiare: "Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui."

[76] Direttiva del parlamento europeo e del consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

La prima normativa unitaria italiana in tema di privacy: L. 675/1996

Il recepimento in Italia di questa direttiva fu quasi immediato, ed avvenne tramite la legge n. 675 del 31 dicembre 1996[77]. È importante tuttavia rilevare come, inizialmente, l'opinione pubblica italiana accettò suo malgrado questa legge. Infatti, come abbiamo avuto modo di riportare, le sentenze ad essa precedenti avevano individuato il diritto alla privacy come un diritto elitario di persone privilegiate che erano sotto gli occhi dei riflettori e reclamavano un diritto d'esser lasciate in pace. Un po' come accadde nell'esperienza americana, anche in Italia la privacy è un diritto che nasce fra i più abbienti e non viene considerato proprio del cittadino comune[78]. La legge 675/96, al contrario, cambia completamente le carte in tavola, immagazzinando al suo interno i dettami comunitari e riconsiderando il diritto su base allargata, finendo con il normativizzare il problema del trattamento dei dati personali nell'era dell' informatica e tutelare in questo modo la totalità dei cittadini.

In aggiunta, al fine di massimizzare tale attività di tutela, sempre su ordine della direttiva[79], è stata istituita la figura del "Garante per la protezione dei dati personali"[80]. Il Garante è un organo collegiale[81] cui sono attribuiti diversi compiti, che avremo modo di approfondire più avanti, ma che tuttavia riveste un ruolo fondamentale poiché, in un certo senso, personifica gran parte dei principi sin ora trattati: controlla che i trattamenti dei dati siano effettuati nel rispetto della legge, riceve ed esamina i reclami e le segnalazioni provvedendo sui ricorsi presentati dagli interessati, vieta anche d'ufficio i trattamenti illeciti o non corretti ed eventualmente ne disponde il blocco, ecc.

---

[77] Legge n. 675 del 31 dicembre 1996, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

[78] Così evidenzia RODOTA' S., *Intervista su privacy e libertà*, *op. cit*., p. 25.

[79] All' Articolo 28 (Autorità di controllo) è stabilito che ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri. L'autorità è pienamente indipendente nelle sue funzioni ed è investita di una serie di poteri (investigativi, effettivi di intervento, ecc).

[80] Istituito con l'art. 30 della suddetta legge, a seguito dell'emanazione del Codice della Privacy, D.lgs 196/2003, e la conseguente abrogazione della L 675/96, è ora disciplinato dall'art. 153.

[81] Costituito da quattro membri, essi sono eletti metà dalla Camera dei Deputati e meta dal Senato, successivamente i componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità: al momento presiede Antonello Soro, mentre prima di lui ci furono Francesco Pizzetti e Stefano Rodotà.

Inoltre il legislatore, superando le aspettative comunitarie, apporta alcune importanti aggiunte rispetto alla direttiva, come il rispetto della dignità personale oltre che dei diritti e delle libertà fondamentali, e la tutela dell'identità personale oltre che della riservatezza[82]. Di conseguenza tale legge ha avuto, per il nostro percorso, una duplice funzione, in quanto ha positivizzato le figure giurisprudenziali del diritto alla riservatezza ed all'identità personale e inoltre ha definitivamente sancito l'importanza, tramite il richiamo alle libertà e diritti fondamentali di dignità della persona, degli sforzi dottrinali e giurisprudenziali che nel tempo si erano susseguiti al fine di costruire modelli certi bisognosi di una specifica tutela. In questo modo, come profetizzato dal giudice Brandeis, essa ha definitivamente messo in chiaro il fatto che il diritto alla privacy altro non è che una porzione di qualcosa di ben più grande, poiché a fronte di un evoluzione tecnologica esponenziale[83], crescono i margini entro i quali una violazione del diritto alla riservatezza diventa possibile, in questo modo la legge abbandona definitivamente la sola concezione negativa del diritto ad essere lasciati soli e ne estende l'operatività alla porzione positiva, regolamentando il controllo attivo dei dati personali e proporzionandolo alle necessità moderne di pubblicizzazione e informazione. In definitiva, si può quindi dire di aver raggiunto una sorta di diritto alla privacy polifunzionale che risponde a molteplici funzionalità e offre una sorta di tutela globale alla persona.

[82] L'art. 1 comma 1 dice che: "La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale."

[83] Non è certo questo il luogo per trattare un elemento di questo tipo, ma non è un mistero che l'evoluzione tecnologico-scentifica non segua schemi lineari bensì esponenziali; gli esperti del settore convergono su una posizione di questo tipo, come ritiene in tema di cd. singolarità tecnologica KURZWEIL R., La singolarità è vicina, Apogeo, 2008.

7. Il Codice della Privacy: D.lgs 196/2003

La ragione di una nuova legge sulla privacy

L'ultima tappa del nostro *excursus* storico alla ricerca di una definizione del concetto di privacy (che, come abbiamo visto, ha diversi significati a seconda del tipo di denominazione) non può che essere il Codice della Privacy, emanato il 30 giugno 2003 col D.lgs n. 196. I motivi che hanno spinto il legislatore ad emanare, a solo sei anni di distanza, una nuova normativa sul medesimo tema della L. 675/96 sono di facile comprensione: subito dopo la legge del 96, furono emanati diversi decreti legislativi, decreti del Presidente della Repubblica e regolamenti di accompagnamento [84] che brevemente trasformarono il panorama legislativo della privacy in una sorta di "giungla giuridica". In aggiunta a ciò, si segnala l'emanazione della direttiva 2002/58/CE, relativa alla vita privata ed alle comunicazioni elettroniche, che quindi rese anche necessario il suo recepimento. Difatti, il Codice della Privacy non muta in alcun modo gli elementi fondamentali della normativa precedente[85] bensì mira a fornire una disciplina approfondita e unitaria, così da cancellare lo spezzettamento normativo dei sei anni antecedenti. In aggiunta, dal momento che il Codice della Privacy sottolinea fortemente, a partire dal titolo, la presenza di un diritto alla protezione dei dati personali, all'interno del più vasto diritto alla riservatezza, bisogna ricordare come questo diritto abbia ricevuto un riconoscimento comunitario all'art. 8 [86] della Carta dei diritti

[84] D.L. n.135, 11 maggio 1999: Disposizioni integrative sul trattamento di dati sensibili da parte dei soggetti pubblici; D.L. n.281, 30 luglio 1999: Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica; D.L. n.282, 30 luglio 1999: Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario; D.P.R. n.318, 28 luglio 1999: Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali; Provvedimento del Garante per la protezione dei dati personali, n.1/P/2000: Individuazione dei dati sensibili da parte dei soggetti pubblici.

[85] Anche perché fare ciò avrebbe comportato necessariamente gravi problemi di tipo comunitario dal momento che, come visto prima, la L. 675/96 è di chiaro influsso comunitario e da tale direttiva non può discostarsi.

[86] Rubricato proprio "protezione dei dati di carattere personale", prevede che "ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

fondamentali dell'Unione Europea, firmata a Nizza il 7 dicembre del 2000. Non manca ovviamente, sempre dal punto di vista comunitario, un riferimento anche al più generale concetto di riservatezza, contenuto nell'articolo precedente[87].

Dal punto di vista strutturale, il Testo unico sulla privacy è strutturato in tre parti e tre allegati[88]; disposizioni generali (artt. 1-45) relativi alle regole fondamentali della disciplina del trattamento dei dati personali, disposizioni particolari per specifici trattamenti (artt. 46-140) ad integrazione o eccezione alle disposizioni generali della parte I e disposizioni relative alle azioni di tutela dell'interessato e al sistema sanzionatorio (artt. 141-186), che analizzeremo, per la parte di diritto penale, in modo approfondito all'interno del Capitolo III.

Nozioni generali

Fornendo ora qualche nozione fondamentale sui temi del Codice, esso prevede che l'interessato, ovvero colui al quale i dati si riferiscono, veda garantito il proprio diritto di accesso a tutte le informazioni su di sé, detenute e trattate da terzi. Infatti, all'art. 7 è prevista la possibilità di conoscere l'autore del trattamento, come e a che fine avviene il trattamento e i soggetti a cui detti dati possono essere ceduti (previo consenso-informato). L'interessato ha facoltà di verificare che i dati siano veritieri in virtù del diritto d'accesso, potendo inoltre richiedere l'aggiornamento o la cancellazione, e, qualora ritenga che gli stessi siano trattati in maniera difforme dalla legge, può chiederne la cancellazione o il blocco. In seguito, se si riscontra una lesione nei diritti sui propri dati, come la raccolta senza il consenso, il consenso acquisito senza aver fornito l'informativa di legge, ecc., si può ricorrere al Garante per la protezione dei dati personali. Inoltre, come anticipato, nei casi più gravi (trattamento illecito dei dati personali, falsità di notificazioni o dichiarazioni al Garante), il bene

[87] Rubricato "rispetto della vita privata e della vita familiare", l'art. 7 della Carta di Nizza prevede che "ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni."

[88] Allegato A, relativo ai codici di condotta; allegato B, concernente il disciplinare tecnico in materia di misure minime di sicurezza; allegato C, sui trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia.

giuridico in questione può essere supportato anche da una tutela penale di rilevante spessore dal punto di vista sanzionatorio.

Il titolo del Codice

Infine, un ultimo appunto va ora riferito circa il titolo del decreto in questione: sebbene in gazzetta sia stato pubblicato col titolo "Codice in materia di protezione dei dati personali", la dizione comunemente utilizzata è quella di Codice o Legge della Privacy[89].Tuttavia quest'ultima, spesso appoggiata ed incoraggiata anche dal primo Garante Stefano Rodotà, per la sua indubbia valenza trasmissiva, non è, dal punto di vista squisitamente giuridico, completamente soddisfacente; essa infatti non riesce a dar conto delle finalità reali ed ermeneutiche della normativa, cioè garantire che il trattamento dei dati personali avvenga all'interno di limiti prestabiliti e non (che è cosa diversa dalle finalità) di difendere la sfera complessiva del diritto alla riservatezza del cittadino.

In un certo senso, aderire alla seconda definizione significa riconoscere nel Codice più una carta sul diritto alla riservatezza, con una sorta di connotato negativo, piuttosto che una legge dalle ripercussioni che derivano dal trattamento dei "dati personali" dell'individuo i quali si pongono, in modo attivo, come conseguenti ripercussioni di un diritto alla privacy.

[89] Questo dibattito trae spunto da Tribunale di Milano, Decreto 27 settembre 1999, n. 600 ove, sebbene relativo alla precedente legge, recante però il medesimo genere di problema, si rinviene quanto segue: "occorre innanzitutto affermare, che la l. 675/96, ancorché conclami in preambolo la "finalità" di garantire il "rispetto dei diritti, delle libertà fondamentali nonché della dignità" della persona, "con particolare riguardo alla riservatezza ed all'identità personale", non può essere né riguardata alla stregua di un vero e proprio "statuto generale della persona" né ritenuta più accentuatamente rivolta alla tutela della persona che alla disciplina sul trattamento dei dati. Simili impostazioni appaiono, infatti, inficiate da un vizio di prospettiva, giacché confondono aspetti diversi e concettualmente infungibili, quali la ratio della normativa e la sua sfera di operatività; aspetti diversi, che solo complementarmente integrandosi concorrono a definire compiutamente il bene giuridico oggetto della tutela accordata: i diritti fondamentali della persona con specifico, ed esclusivo, riferimento alle implicazioni inerenti all'attività di "trattamento di dati personali."

CAPITOLO II – LA TUTELA PENALE DELLA PRIVACY: IL BENE GIURIDICO

1. La nozione di privacy necessaria per la costruzione di un bene giuridico penalmente tutelato: riservatezza e riservatezza informatica - 2. L' «an»: ricerca di una funzione critica del bene giuridico tramite l'analisi della Costituzione - 2.1 L'importanza dell'art. 2 della Costituzione in qualità di norma «aperta»; gli altri articoli della Costituzione - 2.2 La necessità di una tutela penale della privacy alla luce dei suoi risvolti in Costituzione: la funzione di bene giuridico quale «strumentale» o «finale» di tutela3. Il «quomodo»: la struttura di un reato privacy - 3.1 Reati di danno o di pericolo? L'anticipazione della tutela penale - 3.2 L'annoso problema dell'amministrativizzazione del bene giuridico: il rinvio a norme extrapenali e la tutela di funzioni

1. *La nozione di privacy necessaria per la costruzione di un bene giuridico penalmente tutelato: riservatezza e riservatezza informatica*

Al fine di poter affrontare il nucleo di questo elaborato, vale a dire le fattispecie penali che maggiormente risultano problematiche dal punto di vista della tutela della privacy, appare necessario, a seguito dell'evoluzione concettuale portata avanti nel capitolo precedente, tirare le somme e porre ordine sul concetto che ci accingiamo ad approfondire. Infatti, per poter rintracciare in modo sufficientemente esaustivo un bene giuridico all'interno della nostra Costituzione, e valutarne la sua eventuale funzione dal punto di vista della tutela penale, è necessario fornirne dei connotati certi.

La nozione necessaria in Costituzione: una costellazione di diritti

Come visto, il termine privacy, inteso come privatezza o vita privata, può essere sostanzialmente utilizzato in modo analogo al termine riservatezza.

Le sfumature fra i due concetti non possono negarsi[1] e, in parte, sono state affrontate *supra*: probabilmente una accezione leggermente più ampia può essere data alla nozione di riservatezza rispetto a quella di privacy, tuttavia

[1] PATRONO P., voce *Privacy e vita privata (dir. pen.)*, in *Enciclopedia del diritto,* Vol. XXXV, Milano, 1986, 557 e ss. predilige ad esempio l'espressione "vita privata" come sinonimo di privacy, piuttosto che il termine riservatezza, il quale è invece maggiormente apprezzato da MANTOVANI F., *Diritto Penale – Parte Speciale, delitti contro la persona,* Padova, 2012 che ne analizza la valenza duplice di riservatezza informatica e telematica. Fra chi li ritiene fungibili si ricorda MUCCIARELLI F., voce Computer *(disciplina giuridica del) nel diritto penale,* in *Digesto delle discipline penalistiche,* vol II, Torino, 1988, 385 e ss.

entrambe possono identificarsi come figure in grado di assorbire al loro interno diverse sfaccettature. Ambedue accolgono una componente negativa e positiva, già ampiamente trattate, che possono declinarsi in libertà *da*[2] (libertà negativa) e libertà *di*[3] (libertà positiva).

Inoltre, dal momento che grande rilevanza assume, come conseguenza di questi termini, anche l'espressione di "trattamento e protezione dei dati personali", come prevalente esplicazione positiva, ecco che più che mai appare attuale la posizione del Modugno [4] che definisce la privacy come una "*costellazione di diritti, non solo accomunati da caratteri strutturali o formali, quanto piuttosto da una matrice ideale di rifiuto di intrusioni non consentite in una sfera riconosciuta come propria della persona e della sua spontanea socialità*".

Già abbiamo avuto modo di tracciare il significato che il decreto legislativo n. 196 del 2003 riconosce nel trattamento e nella protezione dei dati personali; qui preme rilevare come, a fronte del suo attuale riferimento normativo[5], esso rientri pienamente nel concetto e nel diritto di privacy e, come tale, ha un pieno riconoscimento costituzionale. Questo, come vedremo, sarà un passaggio essenziale per giustificare, relativamente al bene giuridico in questione, talune fattispecie penali. Inoltre, connaturato alla protezione e al trattamento dei propri dati, si instaura, quantomeno in parte, il cd. "diritto all'oblio", inteso come quel diritto della persona di non voler vedere diffusi, senza particolari motivi, precedenti pregiudizievoli su di sé, per tali intendendosi anche i precedenti giudiziari; come ritiene autorevole dottrina[6],

---

[2] Ne riassume alcuni PATRONO P., voce *Privacy e vita privata(dir. pen.)*, cit, 560: diritto ad essere lasciati soli, all'oblio, a mantenere il riserbo su certi dati personali, a limitarne la circolazione.

[3] Il medesimo Autore per il contenuto positivo richiama: l'identità personale, il diritto a trattare i propri dati personali garantito con strumenti quali l'accesso, la rettifica, ecc,.

[4] Si veda MODUGNO F., *I nuovi diritti nella giurisprudenza costituzionale,* Torino, 1995.

[5] Art. 1, diritto alla protezione dei dati personali: "Chiunque ha diritto alla protezione dei dati personali che lo riguardano." E soprattutto art. 2 comma 1, finalità: "Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali."

[6] CERRI A., voce *Riservatezza(diritto alla),* III parte – Diritto Costituzionale, in *Enciclopedia Giuridica Treccani*, Roma, 1999.

esso è definito come il diritto che si esplica per quelle vicende riguardanti una persona che possono essere diffuse negli stretti limiti in cui sono connesse con l'interesse pubblico della notizia (continenza sostanziale) ed i cui modi non eccedano l'intento informativo (continenza formale).

Riservatezza informatica, bene giuridico ulteriore o aggettivazione del precedente?

Tale complesso di argomenti, finora analizzati e sinteticamente evidenziabili nel diritto alla riservatezza (o privacy) non esauriscono tuttavia il novero dei temi necessari per un analisi costituzionalmente orientata. Essi costituiscono infatti una porzione alla quale è possibile contrapporre l'ulteriore concetto di "riservatezza informatica". È infatti indubbio come, a fronte del progresso informatico degli ultimi decenni, ciò che prima era indicato col termine di riservatezza, e che subito poteva far pensare ad ulteriori aspetti come la tutela del domicilio, della segretezza, della corrispondenza e via dicendo, oggi può portare a differenti posizioni, quali la tutela del domicilio informatico, la tutela e la segretezza dei dati personali presenti in banche dati informatiche, e via dicendo. Per averne un evidente riscontro, basterebbe ad esempio confrontare due articoli del Codice Penale quali il 615 bis[7] ("Interferenze illecite nella vita privata") ed il 615 ter[8] ("Accesso abusivo ad un sistema informatico e telematico"), che saranno poi ampiamente ripresi *infra,* per rendersi conto di come quello che a prima vista sembra essere lo stesso bene giuridico tutelato, in realtà assume sfaccettature ben diverse, essendo caratterizzato da evidenti elementi di novità. Il primo rappresenta un concetto classico di privacy, limitatamente alla sua accezione privatistica e del domicilio, per il quale la fattispecie penale è posta a tutela della riservatezza dei propri affari nelle mura domestiche; la seconda invece è costruita (seppure in senso lato) sulla porzione informatica di privacy, per cui la fattispecie è posta a tutela anche di

[7] Si riporta il primo comma: "Chiunque mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'art. 614, è punito con la reclusione da sei mesi a quattro anni."

[8] Si riporta il primo comma: "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo è punito con la reclusione fino a tre anni."

coloro i quali si aspettano che i loro dati personali non siano oggetto di attacchi informatici né siano distrutti o dispersi.

Conseguenza di ciò è che, a seconda delle norme penali prese di volta in volta in considerazione, a cavallo del Codice della Privacy e del Codice Penale, il bene giuridico tutelato potrà rientrare o nella semplice riservatezza, o nella più specifica riservatezza informatica[9]. Tuttavia non è del tutto pacifico se la riservatezza informatica possa essere un ulteriore bene giuridico a sé stante rispetto alla riservatezza, oppure semplicemente l'attributo "informatica" attiene piuttosto alle modalità di lesione di quel bene. In realtà, come vedremo, non sempre è di immediata captazione la presenza di un bene giuridico così netto all'interno di una fattispecie penale; sia perché il bene giuridico tutelato in via primaria è differente, sia perché viene utilizzata la criticata tecnica della tutela di funzioni, ove arretra sensibilmente l'offensività dal bene in questione; in conclusione, le fattispecie che sono effettivamente mirate a tutelare un tale bene in via primaria si riducono inesorabilmente.

[9] Si veda a riguardo VENEZIANI P., in *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali,* tratto da *Il diritto penale dell'informatica nell'epoca di internet,* a cura di L. Picotti, Padova, 2004.

2. *L' «an»: ricerca di una funzione critica del bene giuridico tramite l'analisi della Costituzione*

Giunti al punto di una soddisfacente posizione sull'intendimento circa il diritto alla riservatezza, il passo successivo per il penalista deve essere quello di rintracciare, all'interno della Costituzione, gli appigli normativi che ne giustificano la presenza nel panorama del diritto penale: vale a dire "se" ("*an*"[10]) tale bene giuridico vanti una sufficiente posizione costituzionale da meritare una tutela penale.

I principi guida

In altre parole, in un primo momento è necessario visualizzare quali articoli, in Costituzione, evidenzino la presenza del bene giuridico in questione, come accennato nel precedente capitolo, ed in un secondo momento bisogna porsi il quesito se tali beni giuridici siano di sufficiente riferimento per la costruzione di fattispecie penali. Per rispondere a ciò, risulta necessario vedere se il bene giuridico sia talmente importante, dal punto di vista della protezione costituzionale, da considerarsi necessaria una tutela rafforzata, come quella penale e non, invece, una tutela meno stringente, quale la tutela amministrativa; è necessario capire se, in riferimento al bene giuridico della privacy, valgano i grandi principi del diritto penale quali offensività, sussidiarietà (*extrema ratio),* frammentarietà e così via.

Per quanto riguarda il primo, il diritto penale deve preoccuparsi in chiave repressiva dei soli fatti realmente offensivi di un interesse meritevole di protezione; circa il secondo, è previsto che il diritto penale intervenga, per l'appunto, come *extrema ratio,* e dunque solo quando risultano insufficienti gli altri sistemi sanzionatori del diritto; mentre per il terzo si ritiene che il diritto penale prenda in considerazione non ogni azione lesiva o potenzialmente

[10] Si veda, sui criteri che presiedono alla definizione dell'*an* e del *quomodo* della tutela penale, senza pretese di completezza, ANGIONI F., *Contenuto e funzioni del concetto di bene giuridico,* pag. 163 e ss., Giuffrè, Milano, 1983 o anche, per una posizione più recente, FIANDACA G., *Nessun reato senza offesa*, in G. Fiandaca, G. Di Chiara, *Una introduzione al sistema penale. Per una lettura costituzionalmente orientata*, Jovene, Napoli, 2003.

lesiva di un bene ma solo quei comportamenti che manifestino un cospicuo disvalore.

Così facendo, sarà possibile utilizzare il bene giuridico come punto di riferimento per le scelte di incriminazione, nella sua cd. "funzione critica"[11]. Come è ovvio, un procedimento del genere andrebbe compiuto all'inverso, vale a dire partendo da una fattispecie penale definita, estraendone il bene giuridico, per poi analizzarlo e rintracciare al suo interno il rispetto di tali principi, come dovrebbe fare il legislatore nel momento in cui decide di dare vita ad un nuovo reato. Un' operazione di questo tipo verrà svolta, di volta in volta, quando passeremo in analisi le norme penali di nostro interesse; per il momento possiamo convenire sul fatto che non tutti i reati che andremo ad analizzare soddisfano pienamente tali principi: ad esempio quello di *extrema ratio* o di offensività mal si sviluppa con l'art. 170 del Codice della Privacy ("Inosservanza di provvedimenti del Garante") che, dando luogo ad un evidente fattispecie di tutela di funzioni, probabilmente avrebbe potuto anche essere sviluppato come sanzione amministrativa o quantomeno come contravvenzione piuttosto che come delitto[12].

[11] Si riconoscono diverse funzioni al bene giuridico oltre alla funzione critica, che è la principale, quali la "funzione classificatoria", o la "funzione interpretativa o teleologica", al fine di interpretare correttamente le fattispecie penali. Si veda, a riguardo PAGLIARO A., *Bene giuridico e interpretazione della legge penale,* in *Studi in onore di Francesco Antolisei,* Volume II, Giuffrè. Milano, 1965, p. 391 ss. ed anche MORSELLI E., *In tema di concezione realistica,* in *Problemi generali di diritto penale,* a cura di Vassalli, Giuliano, Giuffrè, Milano, 1982.

[12] Questa posizione è condivisibile in FIORE S., *Riservatezza (diritto alla)*, Parte IV – Diritto Penale, pag. 15, in *Enciclopedia Giuridica Treccani,* Roma, 1998 relativamente al rispettivo art. 37 della L 675/96.

2.1 L'importanza dell'art. 2 della Costituzione in qualità di norma «aperta»; gli altri articoli della Costituzione

Se dunque, come accennato, si vuole rinvenire nel bene giuridico della riservatezza una funzione critica tale da giustificare una normazione penale a tutela di esso, il primo passo da compiere consiste nel ricercare quali articoli della Costituzione siano in grado di ricomprenderlo. Si è già avuto modo di vedere come, grazie ad una costante evoluzione giurisprudenziale, la privacy è stata di volta in volta inserita nell'ambito di quei diritti della personalità che sono espressamente sanciti all'art. 2 della Costituzione: a partire dalla sentenza di Cassazione n. 2129 del 1975, tale diritto è stato definitivamente riconosciuto e legittimato nella nostra Carta Costituzionale la quale, al suddetto articolo, prevede che *"la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale"*[13].

L'art. 2 della Costituzione inteso come norma «aperta»

È noto, infatti, che l'articolo 2 della Costituzione venga universalmente letto come "fattispecie aperta", capace di accogliere al suo interno ulteriori diritti non esplicitamente presenti nella nostra Carta. Questa sua caratteristica "creatrice" fu coniata nel momento stesso in cui i Padri Costituenti forgiarono tale articolo: essi diedero vita ad una Costituzione che fosse in grado di perdurare nel tempo e di evolversi assieme alla società per la quale fu costruita nonché allo sviluppo della persona umana. La dizione utilizzata, volutamente aperta ed ampliabile tramite l'operato della Corte Suprema, ha avuto, infatti, il merito di estrarre nuove fattispecie dal testo della Costituzione, ampliando gli spazi di tutela dei cittadini e degli individui, come testimoniano le

[13] Fra i primi, in dottrina, a sottolineare come l'art. 2 valga ad accogliere il diritto alla riservatezza si veda VASSALLI C., *Libertà di stampa e tutela penale dell'onore* in *Archivio penale,* 1967, mentre, più avanti, si ricorda ROSSI VANNINI A., *La criminalità informatica: le tipologie di computer crimes di cui alla L.547/93 diretta alla tutela della riservatezza e del segreto,* in *Rivista trimestrale di diritto penale dell'economia,* 1994, 436.

numerose decisioni di cui si è occupata[14]. Tali "nuovi diritti"[15] sono stati, in questo modo, in grado di rientrare nel novero dei diritti inviolabili[16] dei quali anche l'art. 2 è portatore, e fra i quali rientra anche il diritto alla riservatezza, espressione del diritto della personalità; a supporto di questa posizione si ricordano anche il disposto dell'art. 12 della Dichiarazione universale dei diritti dell'uomo[17], e dell'art. 8 della Convenzione europea sulla salvaguardia dei diritti dell'uomo e delle libertà fondamentali[18]. Tuttavia, nonostante l'importanza di tale articolo, ve ne sono altri, sempre in Costituzione, che evidenziano come, la riservatezza e la vita privata siano sottoposte ad una tutela stringente anche sotto diversa luce. È pacifico constatare come, sull'art. 2, vi siano ben poche dispute dottrinali sull'accoglimento del diritto alla riservatezza.

L'art. 3 della Costituzione: ulteriore fondamento del diritto?

Discorso ben diverso vale, invece, per l'articolo 3 della Costituzione, analizzato sia in riferimento al I comma, laddove si parla di "pari dignità sociale", sia al II comma, il quale contiene la garanzia del "pieno sviluppo della persona umana", del quale autorevole dottrina[19] ne ha proposto una possibile valenza a fondamento del diritto alla riservatezza. Tuttavia, questa funzione creatrice dell'articolo 3 è stata spesso criticata, in quanto tale

[14] Fra i più importanti si possono ricordare: il "diritto alla vita" (sentenze di cassazione nn. 27 del 1975; 35 del 1997; 223 del 1996), il diritto "all'identità personale" definito come "diritto ad essere se stessi" (sentenza n. 13 del 1994), il diritto alla libertà personale, intesa non solo come garanzia da forme di coercizione fisica della persona, ma che comprende anche la libertà di autodeterminazione del soggetto (sentenza n. 30 del 1962), il diritto d'informazione (sentenze n. 84 del 1969 e n. 348 del 1990), il diritto dell'obiezione di coscienza (sentenze n. 164 del 1985; n. 470 del 1989; e n. 467 del 1991), e così via.

[15] Molto, su questo tema, è stato scritto da questo Autore, cioè BALDASSARRE A., *I diritti fondamentali nello Stato costituzionale*, in *Scritti in onere da Alberto Predieri* Tomo I, Milano 1996.

[16] Si riporta la famosa definizione: "un nucleo che si ritiene sia in ogni caso intangibile ed immodificabile: immodificabile cioè anche di fronte allo stesso potere di revisione costituzionale" di FOIS S., *Questioni sul fondamento costituzionale del diritto alla «identità personale»* , in AA. VV., *L'informazione e i diritti della persona*, Jovene, Napoli, 1983, pp. 161.

[17] Ove si sancisce specificamente che nessun individuo può essere sottoposto ad interferenze nella sua vita privata.

[18] Secondo cui ogni persona ha diritto al rispetto della sua vita privata e familiare.

[19] BRICOLA F., *Prospettive e limiti della tutela penale della riservatezza,* in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Milano, Giuffrè, 1970, p. 84, evidenzia il parallelismo tra l'art. 3 Cost. e gli artt. 1 e 2 della Costituzione tedesca che impiegano formule analoghe a tutela della dignità e dello sviluppo della personalità. Sono queste le disposizioni in cui "la dottrina tedesca ravvisa l'affermazione costituzionale del diritto alla vita privata".

principio, invece, è produttivo solo di "effetti riflessi" sul contenuto dei singoli diritti e solo se ed in quanto essi risultino già specificamente riconosciuti.

La disposizione in esame non potrebbe quindi essere invocata per attribuire valenza costituzionale al diritto alla riservatezza, essendo la sua operatività relegata ad un ambito di secondo grado, una volta risolta positivamente, ma per altra via, la questione dell'esistenza costituzionale del diritto in oggetto. Le critiche però non si fermano qui: alcuni lamentano l'eccessiva genericità della disposizione[20], altri si interrogano sulla reale natura di ostacolo allo sviluppo della persona rappresentato dalla conoscenza di notizie private e dall' attacco alla sfera privata da parte soprattutto dei grandi mezzi di comunicazione di massa[21], altri ancora fanno appello alla marcata dimensione sociale cui l'art. 3 sarebbe ispirato[22] (gli interessi da esso tutelati, dignità e sviluppo della persona, andrebbero visti in un'ottica eminentemente sociale, che non può non contrapporsi alla dimensione individuale in cui si esplicano la vita privata e la riservatezza).

L'esattezza di tali affermazioni deve tuttavia essere ridiscussa alla luce delle nuove caratteristiche del problema in relazione all'avvento della c.d. "società dei computers" e, come precedentemente accennato, alle conseguenti modificazioni a cui il concetto di privacy è andato incontro, per cui non è più possibile, né è opportuna, una netta separazione tra individualità e collettività,

---

[20] FOIS S., *Questioni sul fondamento costituzionale del diritto all'«identità personale»* , in AAVV, *L'informazione e i diritti della persona*, Jovene, Napoli, 1983, p. 167. L'Autore si dimostra contrario all'utilizzazione delle clausole generali dell'art. 3: "il richiamo al valore della persona umana rischia di diventare l'invocazione ad una specie di formula magica per dar forma a fantasmi normativi tali da implicare le conclusioni più diverse e più opposte".

[21] BRICOLA F., *Prospettive e limiti della tutela penale della riservatezza,* in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Milano, Giuffrè, 1970, p. 84. In particolare, secondo l'Autore, «non è provata la correlazione fra violazioni della sfera privata e impedimento al pieno sviluppo della persona umana», ed anzi giunge ad affermare che « una migliore conoscenza della vita privata può giovare ad un migliore inserimento sociale dell'individuo».

[22] MANTOVANI F., *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Milano, Giuffrè, 1970, p. 388 ss. L'Autore riferisce tale opinione per poi criticarla sotto il profilo della contrapposizione troppo decisa tra *civis* e singolo, evidenziando invece l'opportunità di riferirsi alla persona umana integralmente intesa.

se non si vuole incorrere in una falsa e incompleta rappresentazione del problema[23].

La sostanziale sfiducia circa gli articoli 13, 14, 15 e 27 II comma della Costituzione

Proseguendo, sono presenti altre norme, gli articoli 13, 14 e 15, che sanciscono l'inviolabilità della libertà personale, del domicilio, della libertà e segretezza della corrispondenza e ogni altra forma di comunicazione, che possono essere prese in considerazione al fine di attribuire rango costituzionale al diritto alla riservatezza. In questa prospettiva la libertà personale[24] viene intesa non tanto e non solo in senso fisico, ma anche con riguardo alla persona nella sua interezza, ivi compresa la sua sfera spirituale e la sua personalità. Allo stesso modo, domicilio e corrispondenza sono interpretati come proiezione spaziale e spirituale dell'individuo[25]. Per la precisione, la posizione dominante in dottrina afferma che le disposizioni in esame si riferiscono in via primaria a diritti distinti da quello alla riservatezza[26], oppure ad aspetti settoriali e manifestazioni parziali di essa[27], o ancora a diritti qualificati "affini", con particolare riferimento al diritto al segreto[28]. Comunque, come si evince dalle posizioni ora analizzate,

---

[23] Così come sostenuto da S. RODOTÀ , *Tecnologie e diritti*, Bologna, Il Mulino, 1995, pp. 29 ss.

[24] Si ricorda il conciso primo comma: "La libertà personale è inviolabile."

[25] A riguardo si veda G. MORSILLO, *La tutela penale del diritto alla riservatezza*, Milano, Giuffrè, 1966, p. 274.

[26] Sono poche, sebbene Autorevoli, le voci contrarie che sostengono anche in questi articoli un forte appoggio al diritto alla riservatezza: A.M. SANDULLI - A. BALDASSARRE, *Profili costituzionali della statistica in Italia*, in *Dir. soc*., 1973, pp. 382-383, nota 87: « a livello costituzionale, tale diritto è riconosciuto e garantito dagli artt. 13 (che, occorre ripeterlo, si riferisce pure alla libertà personale morale, ossia anche ai beni immateriali inerenti o attinenti alla persona fisica), 14, 15 Cost.».

[27] Ritiene A. BELVEDERE, *Riservatezza e strumenti d'informazione,* in *Dizionario del dir. priv.*, Milano, 1980, p. 750 che "la Costituzione presenta «varie disposizioni che regolano aspetti parziali del problema (talora insieme ad altri interessi), ma che non offrono alcun criterio per formulare una norma generale".

[28] Sull'argomento si veda A. CATAUDELLA, *La tutela civile della vita privata*, Milano, Giuffrè, 1972, p. 27, il quale, nel precisare i caratteri distintivi del segreto rispetto al privato, rileva che, in relazione agli artt. 14 e 15 Cost., sicuramente c'è coincidenza tra ambito del segreto e ambito del privato, ma ciò ha indotto « una parte della dottrina a spiegare tale normativa esclusivamente in chiave di difesa del segreto: "segreto domestico" e "segreto della corrispondenza"». Tuttavia, contro l'assolutezza di tali affermazioni, si deve notare che « non vi è, peraltro, un interesse del soggetto a tenere segreti tutti gli eventi che si verifichino nell'ambito spaziale del domicilio o siano affidati a mezzi riservati di comunicazione». Quindi, a seconda della provenienza delle notizie, il soggetto avrà interesse a limitarne, in misura variabile, la circolazione (notizie riservate), ovvero ad escluderla del tutto (notizie segrete), oppure ancora non si opporrà a consentirne la diffusione. L'Autore, tuttavia, esclude che le norme in esame siano pertinenti al tema della riservatezza, poiché direttamente finalizzate ad impedire non l'indebita divulgazione di notizie riservate ma, più precisamente, il loro apprendimento.

l'atteggiamento piuttosto diffuso che sembra emergere è di una pressoché generalizzata sfiducia verso l'utilizzo delle tre norme in esame come esclusiva àncora costituzionale del diritto alla riservatezza; forse per il timore di indulgere ad operazioni ermeneutiche non sufficientemente supportate da adeguati indicatori di diritto positivo. Tuttavia, certamente, esse assumono una significativa funzione, quanto meno d'appoggio, all'operato principale fornito dall'articolo 2.

Infine, ulteriori appigli cui far riferimento per attribuire garanzia costituzionale alla riservatezza si rinvengono per tramite dell'art. 27, II comma. Questa disposizione sancisce il principio della presunzione di non colpevolezza, cioè l'esigenza e il dovere che l'imputato sia considerato innocente, sia in seno al processo, sia nel contesto sociale, sino alla condanna definitiva. Tuttavia, anche da qui discendono alcune perplessità in quanto manca un definitivo accordo su quale sia l'interesse che la norma mira a proteggere (reputazione e onore o riservatezza in senso stretto), e, in seconda battuta, se essa abbracci solo garanzie di natura squisitamente processuale, oppure si possa estenderne il raggio d'azione, in via mediata, a beni quali reputazione e riservatezza[29]. Qualora comunque si ammetta che la norma in esame copra specificamente la riservatezza, essa tratterebbe un ambito troppo settoriale e particolare, da cui sarebbe azzardato astrarre una tutela di carattere generale. Giunti a questo punto, conclusasi la rapida analisi attraverso la Costituzione, e trovati i fondamenti certi del diritto alla riservatezza, risulta necessario analizzare in che modo essi siano in grado di combaciare con i principi del diritto penale che permetterebbero di fornire loro la tutela che andiamo cercando.

[29] F. MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Milano, Giuffrè, 1970, p. 388, nota n. 9.

2.2 La necessità di una tutela penale della privacy alla luce dei suoi risvolti in Costituzione: la funzione di bene giuridico quale «strumentale» o «finale» di tutela

Dopo aver raggiunto, oltre ad una esaustiva definizione in tema di riservatezza, anche dei solidi appigli costituzionali che garantiscano la presenza di tale bene giuridico nella nostra Carta fondamentale, appare ora necessario chiedersi entro quali limiti la privacy debba essere protetta dal diritto penale. D'altronde, se questa domanda non fosse posta, non sarebbe possibile spiegare per quale motivo il Codice della Privacy distingua, nella sua Parte III[30], Titolo III, un primo Capo denominato "violazioni amministrative" ed un secondo Capo denominato "illeciti penali". Difatti, il primo capo asserisce a quelle violazioni dei dati personali dell'individuo non sufficientemente tali da assurgere ad una tutela penale, bensì solamente a quella amministrativa, ciò in quanto il legislatore ha ritenuto quei comportamenti non abbastanza lesivi del bene giuridico "riservatezza" per quanto riguarda la sua porzione di tutela penale[31]. Il secondo capo, come approfondiremo nel prossimo capitolo, tratta invece nel dettaglio di quelle fattispecie ritenute tali da necessitare un supporto penalistico e che, quindi, riconoscono come il bene giuridico in questione si fonda con i principi cardine del diritto penale. Come anticipato *supra*[32], alcuni dei principi da prendere subito in considerazione, in quanto intrecciati l'un l'altro, sono quello di offensività, sussidiarietà e frammentarietà i quali impongono che il diritto

Le condizioni necessarie perché rilevi una tutela penale della privacy

[30] "Tutela dell'interessato e sanzioni".

[31] Si veda ad esempio l'art. 161 del d.lgs 196/2003 rubricato "Omessa o inidonea informativa all'interessato" il quale prevede che: "La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da seimila euro a trentaseimila euro." In questo caso la violazione dell'art. 13 che prevede, tra le altre cose, l'informazione all'interessato delle finalità e delle modalità del trattamento dei suoi dati, è stata ritenuto, a ragione, solo un illecito amministrativo, poiché la lesione nei confronti dell'interessato del suo diritto al corretto trattamento dei dati personali, non è tale da richiedere l'intervento della disciplina penale. Per approfondimenti si veda proprio su questo tema BANI E., FERIOLI E. A., *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della Privacy"),* a cura di Bianca C. M, Busnelli F. D., Padova, CEDAM, 2007, pagine 2031 e ss.

[32] Si veda il Paragrafo 2 di questo capitolo.

penale si preoccupi in chiave repressiva dei soli fatti realmente offensivi e meritevoli di protezione. Dunque dall'analisi di questi principi discende, in via generale, che il bene giuridico sarà accompagnato da una tutela penalistica soltanto quando l'offesa sia tale da essere fortemente offensiva nei confronti dell'interesse in questione e per cui ogni altro sistema sanzionatorio risulti inappropriato [33]. Tuttavia, non è agevole rinvenire fattispecie penali che soddisfino pienamente questa posizione, in quanto il nostro diritto è caratterizzato da una miriade di sfaccettature anche in ambito sanzionatorio[34] che non permettono sempre di definire come soddisfacente, dal punto di vista della costruzione, una fattispecie penalistica[35]. Alla luce di ciò, è possibile comunque affermare che, a fronte della chiara protezione rintracciata in Costituzione del bene privacy, esista una altrettanto chiara tutela penale, ogni qualvolta il bene giuridico sia aggredito a tal punto da dover rientrare nel principio di offensività. Invece, come avremo modo di vedere più avanti, dubbi a riguardo potranno rilevare nel momento in cui la tutela penale non sia direttamente incentrata nel bene giuridico della riservatezza bensì sia posta a tutela delle funzioni del Garante della Privacy, dando vita alla cd. tutela di funzioni.

Sempre nell'ottica della costruzione di fattispecie penali che vadano il più possibile di pari passo col principio d'offensività per tutelare il bene giuridico in questione, e per fornire inoltre una conclusione soddisfacente in tema di

[33] È questo il concetto delineato dal ROCCO in tema di bene giuridico, che distingue in un primo momento un oggetto giuridico formale da un oggetto giuridico sostanziale: il primo è dato dal diritto dello Stato all'osservanza dei precetti penali mentre il secondo, scindibile in generico e specifico, prevede nel primo caso l'interesse dello Stato all'assicurazione delle condizioni di esistenza della vita in comune, nel secondo caso, si intende il bene o interesse proprio del soggetto passivo del reato, cioè la persona o ente direttamente offeso dal reato e che varia da reato a reato. Così riportato da ANTOLISEI F., *Manuale di Diritto Penale – Parte generale,* Milano, Giuffrè Editore, 2003, pag. 176.

[34] Basti pensare alla tutela di funzioni che sembra porsi, quantomeno sul piano concettuale, in via intermedia fra un reato ed una sanzione amministrativa.

[35] Sul punto ancora ANTOLISEI, ritiene che "il modello classico del diritto penale del bene giuridico rappresenti, più che un connotato dominante della legislazione italiana una costruzione teorica che fa poco i conti con la realtà normativa." In questo modo l'Autore, fa rilevare quanto, sul piano pratico, il dibattito sul bene giuridico tenda ad arrestarsi, dal momento che, alla fine, il penalista deve poi fare i conti con le fattispecie, così come sono prodotte dal legislatore. ANTOLISEI F., *Il problema del bene giuridico,* in *Rivista italiana di diritto penale,* 3, 1939 ed anche FIANDACA MUSCO*, Perdita di legittimazione del diritto penale?*, in *Riv. it. dir. proc. pen*., 1994.

funzione critica di questo bene, risulta necessario mettere a fuoco ulteriormente il discorso in tema di tutela "finale" oppure "strumentale" di quest'ultimo[36]. Si parla di tutela finale di un bene giuridico ogni qual volta tale bene sia direttamente oggetto della tutela penale, e dunque le fattispecie penali mirano a proteggerlo in modo univoco, come accade ad esempio per il patrimonio, tutelato specificamente in Costituzione agli articoli 41 e 42.

Tutela «strumentale» o «finale» del bene giuridico?

Si tratta, invece, di beni strumentali, quando essi siano protetti al fine di assicurare la salvaguardia in via strumentale anche di ulteriori valori; l'esempio classico si ha in tema di diritto penale dell'economia, ove la trasparenza sul mercato degli investitori ha carattere strumentale al fine di tutelare le "tasche" dei risparmiatori e, dunque, il patrimonio[37]. Il punto problematico, su questo tema, si rinviene nel momento in cui l'emersione di beni strumentali comporta un necessario allontanamento dei beni finali dall'orizzonte giuridico dell'oggetto di protezione, e, di conseguenza, dal principio di offensività: difatti non è un caso che a ciò consegua necessariamente l'utilizzo di tecniche di tutela anticipata (quali reati di pericolo astratto o anche solo presunto), dal momento che la lesione di un bene strumentale è solo un pericolo per il bene finale[38]. Bisogna quindi chiedersi se il bene giuridico della riservatezza, così come è stato precedentemente tratteggiato, rientri nel concetto di bene strumentale o finale, al fine di concludere definitivamente il percorso compiuto che ne cerca di delineare il più possibile il suo fondamento nel diritto penale. Per rispondere a questa domanda bisogna rintracciare quegli elementi che fungono da divisori fra

[36] Fra i primi a fornire questa bipartizione si ricorda FIORELLA, *Reato* (Voce), in *Enc. Dir.,* vol. XXXVIII, Milano, 1987 pag. 798 e ss. Egli invita ad accertare che con attenzione che *"l'individuazione di comportamenti illeciti con riferimento ad un bene strumentale che media tutta un'altra serie di beni, i più svariati, non finisca con l'inficiare la determinatezza (sostanziale) della fattispecie e a riflettere se il guardare al bene strumentale faccia perdere completamente di vista l'evento offensivo"*.

[37] Così evidenzia, ad esempio, MUSCO E., MASULLO M. N., *I nuovi reati societari,* Giuffrè Editore, Milano, 2007, pag. 50 e ss. oppure anche, sul problema della carente affidabilità del bene strumentale in tema di offensività, Siracusa L., *La tutela penale dell'ambiente: bene giuridico e tecniche di incriminazione,* Milano, Giuffrè Editore, 2007, pag. 17.

[38] Tale posizione è, fra tanti, analizzata anche in GROSSO C. F., *Introduzione al diritto penale e alla politica criminale*, in *Manuale di diritto penale: parte generale*, Milano, Giuffrè Editore, 2013, pag. 64.

l'uno e l'altro tipo di bene giuridico e che possono riassumersi nei seguenti: un bene di rilievo costituzionale, socialmente apprezzabile, collettivo, materiale e tangibile, cioè consumabile e deteriorabile. È evidente come, riprendendo l'esempio sopra proposto, la trasparenza del mercato difficilmente è in grado di rientrare in alcuni di questi parametri senza l'uso di incomprensibili forzature. Al contrario la privacy, come è stato ampiamente dimostrato, è decisamente un bene di rilievo costituzionale; risulta altresì un bene socialmente apprezzabile, nel momento in cui l'offesa nei suoi confronti sia sufficientemente rilevante; è assolutamente un bene collettivo e, di certo, non più un diritto "dei pochi", come tratteggiato *supra* nel corso dell'*excursus* storico; è, infine, un bene anche materiale e dunque deteriorabile, nel momento in cui la lesione nei confronti dell'individuo avvenga in modo tale da distruggere o disperdere gravemente i dati personali. Da quest'analisi risulta come, indubbiamente, il bene giuridico della privacy possa essere considerato in quanto bene finale e che, dunque, merita una tutela penale decisamente più sofisticata, rispetto ad eventuali beni solamente strumentali[39]. Sicuramente, se una posizione di questo tipo risulta pacifica in tema di reati privacy cd. propri, intesi come quei reati specificamente definiti all'interno del Codice della Privacy, probabilmente meno evidente risulta circa i reati privacy cd. impropri, ovvero quei reati presenti nel Codice Penale e che non sembrano tutelare, almeno direttamente, la riservatezza. La questione sarà approfondita nella singola trattazione di questi reati, tuttavia, nonostante l'argomento risulti almeno all'apparenza spinoso, non vi sono sostanziali problemi a riguardo, dal momento che tali reati, essendo considerati plurioffensivi, abbracciano, in ogni caso, assieme ad altri bene giuridici, anche quello della riservatezza.

[39] Una critica, che si potrebbe muovere a questa posizione, sarebbe quella che riterrebbe il diritto alla riservatezza come mera esplicazione del diritto della personalità (inteso nella sua accezione univoca), e che dunque in questo modo sarebbe solo strumentale al finale bene della personalità. Come però si ha avuto modo di vedere nel primo capitolo, il diritto alla riservatezza ha pieni appigli costituzionali a seguito di numerose sentenze di Cassazione, e dunque non può che considerarsi come diritto a sé stante. L'eventuale critica che, invece, permarrebbe, e che sarà analizzata a breve, sarebbe quella relativa ad alcuni reati del codice della privacy costruiti come tutela di funzioni e che, dunque, mirerebbero a tutelare, più che la riservatezza, la figura del Garante.

3. Il «quomodo»: la struttura di un reato privacy

Giunti a questo punto della trattazione, evidenziate le ragioni che supportano la necessità di una tutela penale nei confronti del bene giuridico della privacy, appare necessario fornire, quantomeno in via generale, le similitudini e le diversità di quei reati che saranno a breve analizzati nel dettaglio, focalizzandosi poi su alcuni dei punti più controversi. Così come è stato analizzato l'*an*[40], è ora indispensabile soffermarsi sul *quomodo*[41], cioè il "come" della tutela penale, così da capire in "che modo" sia costituito un reato privacy.

I diversi tipi di reati privacy

Innanzitutto, è necessario ricordare che possiamo distinguere due diversi tipi di fattispecie penali, le prime, rientranti nel Codice della Privacy, sono denominate reati privacy propri, mentre le seconde, presenti nel Codice Penale, sono definibili come reati privacy impropri. Nel primo caso il reato privacy è proprio, in quanto esplicitamente definito tale dal D. Lgs. 196/2003, e dunque la riservatezza, come bene giuridico, dal punto di vista della tutela penale, rileva in primissimo piano. Per quanto riguarda il secondo caso, a sua volta scindibile in reati privacy impropri informatici e non informatici, il bene giuridico della riservatezza è presente, ma assieme ad ulteriori beni giuridici di medesimo valore costituzionale, dando vita a dei reati dal carattere plurioffensivo[42].

---

[40] Vale a dire se il bene giuridico in questione necessiti di una tutela penale, a cui è stata già data risposta affermativa.

[41] Si rimanda, per i riferimenti bibliografici circa quei criteri che si sviluppano dietro ad una definizione dell'*an* e del *quomodo* della tutela penale, alla nota n. 10 di questo capitolo.

[42] Si tratta, come è ovvio, di quel tipo di reati che offendono non un solo bene giuridico, ma una pluralità di questi; tra gli esempi più noti si ricorda la calunnia (art. 368 cp) che mentre offende lo Stato nel suo interesse ad una amministrazione regolare della Giustizia, lede anche la persona falsamente incolpata. Si noti, tuttavia, che alcuni autori sono contrari alla categoria dei reati plurioffensivi, come PAGLIARO A., *Bene giuridico e interpretazione della legge penale,* in *Studi in onore di F. Antolisei*, II, Milano, 1965, p. 398, nota 16 che ritiene come in realtà il bene tutelato direttamente resta sempre uno solo. Oltre ai reati plurioffensivi ed ai reati monoffensivi si rammenta, infine, anche la presenza di reati cd. ostacolo o di mero scopo, nei quali si incrimina *"non l'offesa di un bene giuridico, ma la realizzazione di certe situazioni che lo Stato ha interesse a che non si realizzino"* come ritiene MANTOVANI F., voce *Colpa*, in *Digesto di diritto penale,* Utet, 1988, vol. II, pag. 301.

All'interno di questo fitto panorama di reati, una ulteriore distinzione da compiere è quella fra delitti e contravvenzioni: mentre nel Codice della Privacy la situazione è piuttosto bilanciata, dal momento che si contano tre delitti e due contravvenzioni[43], nel Codice Penale vi è una preponderanza di delitti contrapposti ad una sola contravvenzione[44]. Il tema è stato ampiamente dibattuto per buona parte del secolo scorso, e diverse teorie[45] sono state elaborate sulla distinzione tra queste due categorie di reato. Fra queste, la teoria maggiormente apprezzata è quella rinvenibile nella Relazione Ministeriale del 1986, che fissa, tra l'altro, alcuni criteri orientativi di massima per la scelta fra delitti o contravvenzioni[46]; di conseguenza, in questo modo, la differenza potrebbe in conclusione rinvenirsi in una semplice diversità quantitativa, secondo la vecchia ed immaginosa espressione del Ferri che definisce le contravvenzioni come "delitti nani[47]". Sostanzialmente le contravvenzioni, rispetto ai delitti, vantano sanzioni minori, essendo punite con l'ammenda e/o con l'arresto, e non con la multa o la reclusione. Esse, inoltre, permettono talvolta la praticabilità dell'oblazione, istituto dagli indiscussi vantaggi, che trasforma il reato in un illecito amministrativo

La differenza fra delitti e contravvenzioni

[43] Fra i delitti abbiamo gli art. 167 (Illecito trattamento di dati), 168 (Falsità nelle dichiarazioni e notificazioni al Garante) e 170 (Inosservanza di provvedimenti del Garante). Tra le contravvenzioni vi sono l'art. 169 (Misure di sicurezza) e l'art. 171 (Altre fattispecie).

[44] Dal momento che la riservatezza, come bene giuridico tutelato, è accompagnata da altri beni quali il patrimonio, il domicilio e l'inviolabilità dei segreti, è semplice capire perché tali reati siano stati configurati come delitti. L'unica contravvenzione è all'art. 734-bis (Divulgazione delle generalità o dell'immagine di persona offesa da atti di violenza sessuale), singolo articolo del titolo II-bis ("Delle contravvenzioni concernenti la tutela della *riservatezza*"), del Capo II, Libro III ("Delle Contravvenzioni"), aggiunto in prima battuta dall'art. 12 della legge n.66 del 1996 e poi rimaneggiato dall'art. 9 della legge n.38 del 2006.

[45] Si veda, nuovamente, ANTOLISEI F., *Manuale di Diritto Penale – Parte generale,* Milano, Giuffrè Editore, 2003, pag. 191 e ss.. Brevemente si riportano, senza pretesa di completezza, le seguenti teorie: *a)* si considerano delitti quei reati che sono caratterizzati da fatti moralmente riprovevoli (*mala in se*) perché offendono la sicurezza del privato e della società, sono contravvenzioni quelle che violano solo leggi destinate a promuovere il pubblico bene (*mala quia prohibita*); *b) "sono delitti quei fatti che producono una lesione giuridica e sono contravvenzioni quei fatti che sebbene possano essere innocenti per se stessi presentano tuttavia un pericolo per la pubblica utilità o per l'altrui diritto"*, così testualmente definite dalla Relazione Ministeriale al progetto del Codice Zanardelli del 5 febbraio 1986; *c)* i delitti sono i reati dolosi o colposi; contravvenzioni i reati per i quali basta la volontarietà dell'azione od omissione.

[46] Criteri secondo i quali la scelta fra delitto o contravvenzione passa per: *a)* norme di carattere preventivo-cautelare per codificare regole di prudenza, perizia, ecc.; *b)* fattispecie concernenti la disciplina di attività sottoposte a un potere amministrativo.

[47] FERRI E., *Sociologia criminale*, 5* ed., vol. II, 1930, pag. 24.

attraverso il pagamento di una somma di denaro, e serve a commutare il reato, accompagnato da una sentenza di proscioglimento per intervenuta estinzione del reato a seguito di oblazione[48], che permette di mantenere pulita la cd. fedina penale[49][50]. Infine, un ulteriore vantaggio delle contravvenzioni è in tema di prescrizione: essa è inferiore per i reati contravvenzionali rispetto ai delitti, poiché quest'ultimi si prescrivono almeno in sei anni, mentre le contravvenzioni in almeno quattro anni[51].

Al fine, ora, di concludere esaustivamente la trattazione sul *quomodo* del bene privacy, è necessario approfondire due ulteriori tematiche precedentemente accennate: il problema dell'anticipazione della tutela penale, a cavallo fra i reati di danno e di pericolo, e quello della tutela di funzioni e della normativa extrapenale con la conseguente amministrativizzazione del bene giuridico.

[48] Spesso si dice, nelle aule di giustizia, che il reato è "oblabile": in tema di contravvenzioni privacy, l'oblazione non è possibile per l'art. 734-bis cp. (prevede il solo arresto), mentre nel d.lgs, 196/2003, l'unico reato oblabile è all'art. 171. La critica principale mossa al sistema dell'oblazione è quella di disegnare maggiormente il sistema penale come un sistema troppo blando dal punto di vista del sistema sanzionatorio: si veda ad esempio, in tema di oblazione nei reati ambientali, la posizione di RAMACCI L., *Diritto penale dell'ambiente,* CEDAM, Padova, 2009, pag. 91 e ss.

[49] L'oblazione può essere di due tipi, obbligatoria (quando la contravvenzione è punita con la sola ammenda) o facoltativa[49] (quando è punita alternativamente con arresto o ammenda): nel primo caso, il giudice, nei casi previsti dalla legge, è tenuto a concederla obbligatoriamente, mentre, nel secondo caso, il giudice la concede a seguito di una personale valutazione sulla gravità del fatto. Da ciò ne consegue che il reato sarà "oblabile[49]" solo nel caso in cui la contravvenzione non sia punita congiuntamente dall'arresto e dall'ammenda, o dal solo arresto, altrimenti l'alternativa resterà il decreto penale di condanna.

[50] Termine volutamente atecnico e di linguaggio comune, ma di immediata captazione, indica il registro penale nel quale sono annotate le condanne definitive di un soggetto, tecnicamente denominato "Certificato del casellario giudiziale". Si ricorda inoltre, per completezza, che l'oblazione va tenuta distinta dal decreto penale di condanna, che anch'esso permette, col pagamento di una somma di denaro, la più rapida conclusione di un procedimento penale nei casi prescritti dalla legge. Esso, tuttavia, porta comunque a "sporcare la fedina penale", in quanto in tal caso il reato non si estingue come nell'oblazione.

[51] Così come previsto dalla legge "*ex Cirielli*" n. 251 del 2005 che ha modificato il tema della prescrizione contenuto nel codice penale.

3.1 Reati di danno o di pericolo? L'anticipazione della tutela penale

La discussione in tema di anticipazione della tutela penale, esistente da molti decenni[52], si articola ogni qualvolta ci si chieda, in tema di offensività al bene giuridico in questione, sino a che punto la fattispecie penale sia costruita a protezione dell'interesse protetto, vale a dire sino a che punto la stessa fattispecie stimoli il principio d'offensività al fine di garantire la tutela di detto bene. Dunque, sempre in tema di *quomodo* sul bene privacy, risulta necessario fornire uno schema esemplificativo che ricomprenda per categorie detti reati, sviluppato sui diversi gradi di offensività che questi ultimi propongono, così da ricevere una visione di insieme.

Reati di danno o di pericolo

Tuttavia, a premessa di ciò, urge fornire alcune delucidazioni generali sul tema. La distinzione fra i reati di danno e di pericolo prende essenzialmente di mira quel pregiudizio che è inerente al fatto criminoso e dunque, come accennato, l'offesa al bene protetto. L'effetto immediato che deriva da un azione criminosa può concretizzarsi in un pericolo oppure un danno a tale bene. Dunque considerando il momento in cui un certo reato si perfeziona, bisogna accertare se tale fatto che integri il reato costituisca una lesione o una semplice esposizione a pericolo dell'interesse protetto. Di conseguenza si ritiene siano di danno quei reati che si perfezionano nel momento in cui il bene tutelato sia distrutto o diminuito, mentre saranno di pericolo quelli per i quali è sufficiente che il bene sia minacciato[53]. Come si sarà intuito a seguito di questa breve distinzione, tale ultima categoria di reati implica un'anticipazione della tutela penale, dal momento che si protegge un determinato bene giuridico per il solo fatto di essere stato messo in una situazione di potenziale pericolo e non per essere stato oggetto di danneggiamento o diminuzione.

[52] Fra gli studi sul tema, tra i più datati, si ricordano DELITALA, *Reati di pericolo,* in *Studi in onore di B. Petrocelli,* v. III, Milano 1972, pag. 1731 e ss. o anche PATALANO, *Significato e limiti della dommatica del reato di pericolo,* Napoli, 1975, pag. 67 e ss.

[53] Un classico esempio solitamente riportato per i reati di pericolo è quello dell'art. 276 c.p. ("Attentato contro il Capo dello Stato"), che si consuma semplicemente tramite il compimento di un atto diretto contro la vita, l'incolumità o la libertà personale dello stesso, mentre il tipico esempio del reato di danno è l'omicidio, che per consumarsi necessita la distruzione della vita di un uomo.

Quest'anticipazione di tutela, decisamente ritenuta necessaria all'interno della categoria dei reati di pericolo, relativamente a tutti quei beni giuridici che per la loro particolare complessità e fragilità abbisognino di una tutela più stringente e ferrea[54], è stata tuttavia criticata da una parte della dottrina all'interno dell'ulteriore distinzione, nei reati di pericolo, fra reato di pericolo concreto, astratto e presunto[55]. Per quanto riguarda i primi, si ritiene si tratti di quei reati in cui il pericolo è elemento (esplicito od implicito) del fatto tipico e dunque il giudice dovrà accertare, *ex ante,* se nel singolo caso concreto il bene giuridico ha corso un effettivo pericolo; circa i secondi, si intendono quei reati nei quali il legislatore, sulla base di leggi di esperienza, ha ritenuto che una classe di comportamenti sia fonte di pericolo per uno o più beni giuridici, quindi il pericolo è la *ratio* dell'incriminazione, ma non è elemento del fatto tipico di reato[56]; i terzi, infine, comprendono quei reati per i quali l'autore del fatto, al contrario dei reati di pericolo astratto, non è ammesso a provare l'inesistenza del pericolo in quanto esso stesso è presunto *iuris et de iure*[57].

Pericolo astratto e presunto alla luce del principio di offensività

Nonostante la distinzione fra gli ultimi due non sia pacifica in dottrina, è stato correttamente rilevato che, soprattutto per quanto riguarda i reati di pericolo astratto e presunto, a causa di una aggressiva anticipazione della tutela penale, il principio di offensività risulta fortemente corroso, dal momento che, in alcuni casi, si vanno a costruire delle fattispecie penali ben lontane dal bene

[54] Si è ritenuto, infatti, che la minaccia di una pena collegata alla (mera) esposizione a pericolo di un bene sortisce, infatti, un effetto di intimidazione/deterrenza ulteriore e, quindi, superiore a quello espresso dalle fattispecie di danno.

[55] La posizione, sul tema, non è univoca, si veda infatti ANTOLISEI F., *Manuale di Diritto Penale – Parte generale,* Milano, Giuffrè Editore, 2003, pag. 266 il quale ritiene che dietro alla distinzione fra pericolo astratto e concreto si annidi un equivoco: "*il concetto di pericolo astratto è inammissibile perché se il pericolo è probabilità di un evento temuto, non si può concepire una species di pericolo in cui questa probabilità manchi. Il pericolo in conseguenza è sempre concreto e ne deriva che nei casi in cui si ravvisa un pericolo astratto in realtà si ha una presunzione di pericolo che non ammette prova in contrario".* In questo modo, l'Autore ritiene che la tripartizione proposta vada sostituita con la semplice bipartizione fra i reati di pericolo concreto ed i reati di pericolo presunto.

[56] A titolo di esempio, per fornire la differenza pratica fra un reato di pericolo astratto ed uno concreto, si veda l'art. 423 del codice penale ("Incendio"), per il quale al primo comma si evidenzia un caso di pericolo astratto (ove non è richiesta l'analisi del giudice), e nel secondo si tratta di pericolo concreto, dal momento che è richiesta l'analisi del giudice "*se dal fatto deriva pericolo per l'incolumità pubblica"*.

[57] Esempio di tale tipologia di fattispecie penale è il delitto di detenzione o di porto illegale di armi.

giuridico che mirano a tutelare e che possono giustificarsi solo come scelte politiche del legislatore[58]. Di conseguenza il rischio è quello di dar vita a dei reati che avvicinano sin troppo il momento in cui la fattispecie dovrebbe perfezionarsi, vanificando, in questo modo, il significato più profondo del principio di offensività.

Ritornando più prettamente al tema della nostra trattazione, è possibile rintracciare sia reati privacy costruiti attorno allo schema del reato di danno sia a quello di pericolo concreto e astratto, ma non di pericolo presunto.

Tra i più interessanti, che presto avremo modo di trattare, figura l'art. 167 del Codice della Privacy ("Trattamento illecito dei dati"), che è costruito come reato di pericolo concreto. Infatti, rispetto al suo antecedente della legge n. 675 del 96, che era sviluppato come reato di pericolo presunto[59], l'art. 167 propone uno schema per il quale il giudice è chiamato ad analizzare se "dal fatto deriva nocumento", dando vita ad un ulteriore e maggiore tipicizzazione del danno e del profitto del reato[60]. Invece, un esempio fra i reati di pericolo astratto è rinvenibile nell'art. 615-ter del Codice Penale ("Accesso abusivo ad un sistema informatico o telematico") il quale prevede che la sola introduzione in tale sistemi dia vita al reato in questione[61]. In tema invece di reato di danno, per il quale il principio di offensività risulterà certamente stimolato nel suo significato più profondo, sicuramente rileva l'art. 640-ter del Codice Penale ("Frode Informatica"), il quale si perfeziona nel momento in cui chiunque alterando un sistema informatico o telematico procura per se o per altri un ingiusto profitto con altrui danno.

---

[58] Le critiche mosse dalla dottrina su tali reati non sono poche, tuttavia essi continuano comunque ad essere in aumento negli ordinamenti degli stati moderni. Fra questi autori si citano GRASSO, *L'anticipazione della tutela penale: i reati di pericolo ed i reati di attentato*, in *Riv. it. dir. proc. pen.*, 1986, 689 ss; PARODI GIUSINO, *I reati di pericolo tra dogmatica e politica criminale,* Milano, 1990, pag. 3.

[59] Si trattava dell'art. 35 L. n. 675 del 1996.

[60] Questo punto è stato approfondito tramite sentenza di Cassazione Penale sezione III del 9 luglio del 2004 e che più avanti sarà trattato nel dettaglio, studiata da Sica S., *Danno e nocumento nell'illecito trattamento di dati personali,* in *Il diritto dell'informazione e dell'informatica,* n. 4-5, 2004.

[61] In questo senso si veda FONDAROLI, *La tutela penale dei "beni informatici"*, in *Il diritto dell'informazione e dell'informatica,* 1996, pag. 311.

3.2 L'annoso problema dell'amministrativizzazione del bene giuridico: il rinvio a norme extrapenali e la tutela di funzioni

A conclusione dell'analisi sul bene giuridico della riservatezza, è giunto ora il momento di porre l'attenzione su quel tema, già più volte accennato, della tutela di funzioni, con il conseguente rischio dell'amministrativizzazione del bene giuridico e del distaccamento dal principio di offensività. Quest'argomento, sebbene non sia rilevante per quanto riguarda i reati privacy impropri del Codice Penale, i quali non prevedono la tutela di funzioni o richiami alla normativa extrapenale, è fortemente attuale relativamente al Codice della Privacy che, in ognuno degli articoli relativi alla disciplina penalistica, prevede faticosi richiami ad altri articoli dello stesso codice per la costituzione delle fattispecie, spesso indirizzati non solo a tutela della riservatezza, ma anche della figura Garante della Privacy.

I limiti del richiamo alla normativa extrapenale

Partendo dal problema del richiamo alla normativa extrapenale, il quesito classico che ci si pone è il seguente: può la norma penale rinviare alla violazione di altri rami dell'ordinamento? Il rischio, che tale condotta porta sempre in seno, è quello di non delineare con sufficiente precisione e tassatività il comportamento vietato, dal momento che, inoltre, la norma extrapenale può essere sempre oggetto di interpretazione analogica, cosa che, invece, per il diritto penale è assolutamente vietata, come previsto dall'art. 14 delle disposizioni sulla legge in generale. Solitamente, la scelta del rinvio a norma extrapenale è compiuta soltanto quando è assolutamente necessario il rinvio ad alcune norme di carattere tecnico [62] che risultano essenziali e inevitabili per la costruzione di una fattispecie penale. Un esempio comune, nel quale si rinvengono problemi di questo tipo, è il diritto penale

[62] Su questo tema, si veda ad esempio, in ambito di diritto penale dell'ambiente, la posizione di SIRACUSA L., *La tutela penale dell'ambiente: bene giuridico e tecniche di incriminazione,* Milano, Giuffrè Editore, 2007, pag. 136 e ss la quale sottolinea come il richiamo alla normativa extrapenale in tema di reati ambientali risulta necessaria dal momento che gli articoli richiamati individuano alcune caratteristiche tecniche senza le quali la costruzione della fattispecie sarebbe impossibile.

dell'economia, riconosciuto come un tradizionale settore di crisi del bene giuridico[63]. In casi di questo tipo, tali scelte di penalizzazione comportano necessariamente una perdita del coefficiente personalistico, con ciò, il reato perde "*la visibilità del male: il controllo penale cessa di essere una risposta ad azioni malvagie e tendenzialmente diventa una protezione collaterale del diritto amministrativo*"[64]. Per quanto concerne il Codice della Privacy, non è presente nemmeno uno, tra gli illeciti penali ivi previsti, nei quali manchi un richiamo ad un articolo del medesimo codice. Di certo, come si vedrà nell'analisi di ogniuno di questi reati, la maggior parte dei rinvii risulta necessariamente inevitabile, poiché, come si è detto, trattandosi di aspetti prevalentemente tecnici, lo sviluppo di una fattispecie completa, senza la presenza di tali richiami, sarebbe risultata eccessivamente complessa, se non addirittura impossibile, all'interno di una sola disposizione[65]. Risulta comunque ovvio come, alla luce di una complessa e sempre mutabile analisi della normativa extrapenale, disposizioni di questo tipo difficilmente rimangono ancorate al concetto di *extrema ratio* e dunque, di conseguenza, sono costrette ad arrancare nel momento in cui si cerca di trovare in esse un fondamento concreto del bene giuridico che mirano a tutelare. Se dunque, per un verso, il rischio dell'amministrativizzazione del bene giuridico, con conseguente perdita di tassatività, si può concretizzare di fronte a quelle fattispecie che portano in seno norme extrapenali non sufficientemente tecniche da lasciare eccessivi spiragli interpretativi, per altro verso, lo stesso problema può rintracciarsi sotto una diversa angolazione, vale a dire quella per

[63] PARODI G., *I reati di pericolo tra dogmatica e politica criminale*, Milano, 1990, 54. Parte della dottrina accosta a questi reati il modello dei cosiddetti reati *victimless*: PALIERO, *Consenso sociale e diritto penale*, in *Riv. it. dir. proc. pen*., 1992, 915 s. Famoso è l'art. 2629-bis del Codice civile, rubricato "Omessa comunicazione del conflitto di interessi"; in questo caso la fattispecie criminosa è completamente traslata all'interno del richiamato art. 2391 II comma cc, creando non pochi problemi dal punto di vista interpretativo.

[64] Come analizzato da HASSEMER, *Il bene giuridico nel rapporto di tensione tra Costituzione e diritto naturale*, in *Dei delitti e delle pene*, 1984, pag. 110 e ss.

[65] Ad esempio, all'art. 169 ("Misure di sicurezza") è previsto che: Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni." L'art. 33 a sua volta, per essere compiutamente individuato, si sviluppa tramite il rinvio a due ulteriori articoli del Codice, così che la definizione normativa di "misure minime" risulta eccessivamente difficile, in quanto a cavallo tra diversi articoli.

cui una fattispecie sia costruita maggiormente a tutela di un organo di vigilanza o di controllo, piuttosto che a tutela del bene giuridico che si aspetterebbe essere coperto. Si tratta di quell'insieme di reati nei quali il bene giuridico tutelato non è più finalisticamente, quello che la fattispecie sarebbe tenuta a tutelare, bensì, in via strumentale, un diverso bene giuridico, costruito *ex novo* sull'organo oggetto di tutela il quale, a sua volta, esercita attività di tutela nei confronti del bene giuridico originario[66]. Secondo una celebre posizione dottrinaria[67] questi reati con offesa funzionale ineriscono a "luoghi giuridici", nei quali sono ricompresi una vastità di interessi eterogenei il cui contemperamento è affidato ad un'autorità pubblica, reprimendo dunque condotte disfunzionali rispetto ad esigenze di controllo espresse da una normativa diversa da quella penale. In questo modo, ricollegandoci al problema della normativa extrapenale affrontato *supra*, l'offesa consiste proprio nella violazione delle modalità stabilite dalla stessa normativa extrapenale di riferimento per lo svolgimento di una certa attività. Il collegamento col discorso circa la labilità del principio d'offensività è presto fatto, nel momento in cui ci si accorga di come, sviluppando delle fattispecie in questo senso, si dia vita necessariamente a reati di pericolo astratto o addirittura presunto nei confronti di tali organi di vigilanza che di conseguenza, come si ha avuto modo di affrontare nello scorso paragrafo, ledono e non poco il suddetto principio. In conclusione, ciò che appare evidente è che, in realtà, l'utilizzo dello schema dei reati di pericolo astratto o

Il significato della tutela di funzioni: ulteriore depauperamento al principio di offensività

[66] Si riporta, come esempio, sempre in tema di diritto penale dell'economia, l'art. 170 bis del Testo unico della Finanza ("Ostacolo alle funzioni di vigilanza della CONSOB") per il quale è punito chiunque ostacola le funzioni di vigilanza attribuite alla CONSOB. In questo caso, il bene giuridico non è più, come per la maggior parte dei reati societari, il patrimonio degli investitori, bensì il "corretto funzionamento del mercato", costruito sopra la figura dell'organo della CONSOB, che si sviluppa come bene strumentale e non più finale a tutela del patrimonio. Nel dettaglio su questo tema si ricorda SGUBBI, FONDAROLI, TRIPODI, *Diritto penale del mercato finanziario,* II edizione, CEDAM, Padova, 2013 pag. 259 e ss.

[67] PADOVANI, *Diritto penale della prevenzione e mercato finanziario*, in *Rivista it. Dir. proc. Penale*,1995, pag. 81 e ss.

presunto viene, in questi casi, riferito proprio a beni giuridici immateriali (cioè i sopracitati beni funzionali costruiti sugli organi di vigilanza), rispetto ai quali l'identificazione di un momento offensivo inteso naturalisticamente risulta oltremodo difficoltosa o, addirittura, non riconducibile ad una singola condotta illecita: si ricade, in questo modo, in un'anticipazione dell'anticipazione[68], il che equivarrebbe di fatto a dire che il coefficiente offensivo di tali fattispecie si fa sempre meno percepibile[69].

Le possibili soluzioni del problema in tema di reati privacy

Venendo ora all'applicazione di tale problematica all'interno del bene giuridico della privacy, è possibile notare, ancora una volta, che il problema della tutela di funzioni è presente nel solo Codice della Privacy e non nei reati impropri all'interno del Codice Penale. Il problema si ha con riferimento all'art. 170 del Codice[70] ("Inosservanza di provvedimenti del Garante"), circa il quale, già relativamente al suo antecedente cronologico della legge n. 675 del 1996[71], se ne era criticata la sua formula a tutela dell'organo del Garante. È evidente come questo reato sia costruito a tutela della funzione di controllo, propria dello stesso organo, dando vita ad una marcata anticipazione delle incriminazioni ed al successivo già citato impoverimento dell'offensività. Di conseguenza, soprattutto secondo parte di una dottrina risalente ad un periodo di poco antecedente alla legge n. 675 del 1996, fattispecie di questo tipo andrebbero tipizzate invece quali illeciti amministrativi, in quanto si riteneva

---

[68] Questo pensiero è rinvenibile nel già citato GRASSO, *L'anticipazione della tutela penale: i reati di pericolo ed i reati di attentato*, in *Riv. it. dir. proc. pen*., 1986, pag. 710 e ss.

[69] Senza pretese di completezza, sul tema della tutela di funzioni e dell'anticipazione dell'anticipazione, molti sono gli autori che si sono pronunciati fra cui COCCO, *Beni giuridici funzionali* versus *bene giuridico personalistico,* in *Studi in onore di Giorgio Marinucci,* a cura di Dolcini e Paliero, Milano, 2006, pag. 167; ZUCCALÀ, *Due questioni attuali sul bene giuridico: la pretesa di dimensione critica del bene e la pretesa necessaria offesa ad un bene,* in *Riv. Trim. dir. pen. Ec.,* 2004, pag. 839 e ss.; Moccia, *dalla tutela di beni alla tutela di funzioni: tra illusioni postmoderne e riflussi illiberali,* in *Riv. It. Di dir. e proc. Pen.,* 1995, pag. 343 e ss.

[70] "Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2 e 143, comma 1lettera c), è punito con la reclusione da tre mesi a due anni."

[71] Addirittura, si fa notare, il dubbio circa lo sviluppo di tale reato a tutela di funzioni fu palesato già nel lontano 1984 nel "Progetto Mirabelli", per la difficoltà di individuarne il bene protetto mancando la protezione ad interessi concreti quale la privacy e diventando una mera disobbedienza ad un precetto. In questo senso a quel tempo si ricorda PECORELLA G., *Profili penalistici della regolamentazione delle banche dati,* in *AA. VV., Le banche dati in italia. Realtà normativa e progetti di regolamentazione* (a cura di V. Zeno-Zencovich), Napoli, 1985, pag. 147 e ss.

che "*l'illecito amministrativo ben possa essere previsto in dipendenza di violazioni di un obbligo di fare, quindi di carattere omissivo e quindi in definitiva di violazioni di carattere procedimentale, che, a ben considerare, non ledono né mettono in pericolo alcun concreto bene giuridico ma solo disturbano la regolarità del procedimento di elaborazione dei dati*[72] ". Tuttavia, sulla falsa riga del già affrontato discorso relativo ai beni giuridici strumentali e finali, non manca chi ritiene che si possa enucleare un nuovo bene giuridico rappresentato dalla cd. "intangibilità informatica" che indica la "*multiforme esigenza di non alterare la relazione triadica tra dato della realtà, rispettiva informazione e soggetti legittimati ad elaborare quest'ultima nelle sue diverse fasi (creazione, trasferimento e ricezione)*[73] ", giustificando in questo modo una fattispecie penale quale l'inosservanza dei provvedimenti del Garante. Infine non manca chi, cercando di mediare, ritiene come "*in questo campo una ragionevole linea di coordinamento fra sanzione penale e sanzione amministrativa potrebbe essere tendenzialmente tracciata a seconda che la violazione consista nell'inosservanza di obblighi strumentali al controllo specifico e puntuale di un attività già denunciata all'autorità ovvero consista in una tutale elusione del controllo di quest'ultima: mentre la prima ipotesi potrebbe essere il regno delle sanzioni amministrative, per la seconda non sarebbe da escludere il ricorso alla sanzione criminale*"[74].

Di conseguenza, sebbene il problema rimanga tendenzialmente aperto, ed in ogni caso irrisolvibile fino a nuovo ed eventuale intervento del legislatore, sposando quest'ultima ipotesi sarebbe tuttavia possibile convivere, quanto meno sul piano dei principi generali del diritto penale, colla presenza di un reato sviluppato sul sistema della tutela di funzioni.

---

[72] Così riteneva MANNA A., *La protezione personale dei dati personali nell'ordinamento italiano,* in *Rivista trimestrale di diritto penale dell'economia,* 1993, pag. 188 e ss.

[73] Secondo la posizione di MILITELLO V., *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni,* in *Rivista trimestrale di diritto penale dell'economia,* 1992, pag. 374 e ss.

[74] E' la posizione condivisa da PALAZZO F.C., *Bene giuridico e tipi di sanzione,* in *Indice Penale,* 1992, pag. 227 e ss.

CAPITOLO III – I REATI PRIVACY PROPRI: IL CODICE PRIVACY

1. Gli illeciti penali nel codice privacy: i reati privacy propri - 1.1 Trattamento illecito di dati: premessa (art. 167) - 1.1.1 La violazione della normativa richiamata e le sue criticità - 1.1.2 Nozione del termine «trattamento», condotta e ratio della tutela - 1.1.3 Ulteriori elementi strutturali del reato e clausola di riserva - 1.1.4 Risvolti pratici all'interno dell'attuale realtà informatica: il caso Vividown e l'impatto sui social network - 1.2 Falsità nelle dichiarazioni e notificazioni al Garante (art. 168) - 1.3 Misure di sicurezza (art. 169) - 1.4 Inosservanza di provvedimenti del Garante (art. 170) - 1.5 Altre fattispecie (art. 171)

1. Gli illeciti penali nel codice privacy: i reati privacy propri

Secondo la suddivisione sinora adottata, i reati contro la privacy propri[1] sono quelli presenti all'interno della Parte Terza, Titolo III del D.lgs n. 196 del 2003, conosciuto come "Codice della Privacy"[2], ricompresi tra gli articoli 167 e 171. Come si è già accennato nel corso di questo elaborato, il legislatore ha deciso di riservare sanzioni penali alle più gravi violazioni relative all'istituto del consenso, al trattamento dei dati personali, agli obblighi di notificazione, dando vita a tre delitti e due contravvenzioni[3]. Per quanto riguarda l'art. 172[4], ultimo articolo del Titolo III, esso prevede invece la pena accessoria della pubblicazione della sentenza come conseguenza per la condanna di uno dei due delitti.

[1] Da tenere distinti rispetto ai reati privacy impropri, dei quali si tratterà nel capitolo seguente, all'interno del Codice Penale.

[2] Anche se, come si è ampiamente dimostrato alla fine del I Capitolo, la dizione corretta rimane quella con la quale il decreto è stato promulgato in Gazzetta Ufficiale: "Testo unico sulla privacy e sul trattamento dei dati personali".

[3] Si ricorda che tra i delitti abbiamo gli art. 167 (Illecito trattamento di dati), 168 (Falsità nelle dichiarazioni e notificazioni al Garante) e 170 (Inosservanza di provvedimenti del Garante). Tra le contravvenzioni vi sono l'art. 169 (Misure di sicurezza) e l'art. 171 (Altre fattispecie).

[4] "Pene accessorie": La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza. E' peculiare il fatto che la pubblicazione sia imposta indipendentemente dal comportamento criminoso avvenuto in concreto, senza che il giudice possa valutarne la necessità caso per caso, limitandone magari l'uso ai casi più gravi. Più che altro, il controsenso sarebbe rinvenibile nel momento in cui la pubblicazione avrebbe effetto controproducente anche verso la vittima del reato, che potrebbe vedersi costretta a subire un altro intervento lesivo della sua privatezza.

Inoltre, i reati qui in esame sono da considerare anche come "eventualmente informatici"[5], infatti la loro consumazione può, in certi casi, prescindere dall'abuso di sistemi informatici o telematici: il trattamento illecito dei dati, ad esempio, ben può compiersi anche col semplice sussidio di supporti cartacei, quando è effettuato in violazione della norma del Codice che prevede il consenso (art. 23), senza necessariamente richiedere strumenti elettronici. L'omessa adozione delle misure minime di sicurezza, invece, è un reato informatico in senso stretto, in quanto per perfezionarsi, prevede la violazione dell'art. 33 per il trattamento elettronico dei dati.

Le principali differenze fra normativa attuale e normativa previgente

Si ricorda, inoltre, che prima del presente decreto legislativo, la normativa vigente era quella contenuta nella L. 675/96 che, a sua volta, accoglieva, dall'art. 37 all'art. 39-bis, delle fattispecie penali sulle quali sono poi stati ricalcati i reati in oggetto. Tuttavia, al giorno d'oggi, non compare più la vecchia fattispecie di omessa o incompleta notificazione, la quale compariva all'art. 35 della L. 675/96, e che è stata invece depenalizzata, diventando un semplice illecito amministrativo. Parte della dottrina[6] ha, infatti, insistito sul principio di sussidiarietà del precetto penale e di necessaria lesività della condotta incriminata; in questo modo si è proposta una differente graduazione anche sotto il profilo qualitativo del reato, così da diversificare la sanzione in relazione al particolare disvalore del fatto illecito. In poche parole, ricollegandoci agli aspetti più critici affrontati *supra*, furono accolte quelle correnti dottrinarie che palesavano (non solo per questo reato), un *deficit* di offensività ed un utilizzo del precetto penale in chiave meramente sanzionatoria di disposizioni extra-penali. Di conseguenza, sono state però

[5] L'utilizzo di questa dizione è rinvenibile in LUBERTO M., *I reati informatici contro il diritto alla privacy. La tutela fornita dal D.lg. n.196 del 2003 e dal Codice Penale,* in *Giurisprudenza di merito,* 2008, 3, pag. 900 e ss.

[6] Ciò anche in seguito di alcune critiche dottrinarie quali VENEZIANI P. *Beni giuridici protetti e tecniche di tutela penale,*in *Rivista trimestrale di diritto penale dell'economia,* 1997, pag. 166 e soprattutto MANNA A., *La protezione penale dei dati personali nel diritto italiano,* in *Rivista trimestrale di diritto penale dell'economia,* 1993, pag. 188 il quale ritiene che "*l'illecito amministrativo ben possa essere previsto in dipendenza di violazioni di un obbligo di fare, quindi di carattere omissivo (proprio), cioè, in definitiva, di violazioni di carattere 'procedimentale', che, a ben considerare, non ledono, né mettono in pericolo alcun 'concreto' bene giuridico, ma solo 'disturbano' la 'regolarità' del procedimento di elaborazione dei dati*".

inasprite, rispetto alla precedente legge, la maggior parte delle sanzioni amministrative, ritenute sino a quel momento non sufficientemente in grado di fornire un efficace deterrente, considerando le posizioni economiche di alcuni titolari dei trattamenti dei dati.

Un'ulteriore novità da segnalare rispetto alla antecedente legge in tema di trattamento dei dati concerne l'oggetto e l'ambito di applicazione di tutta la normativa in esame. L'art. 5 del Codice Privacy prevede, infatti, la regola della vigenza della legge italiana a prescindere dal luogo nel quale si trovi l'archivio dei dati personali del titolare del trattamento, che potrebbe tranquillamente avvenire all'estero, indipendentemente dalla nazionalità o dal luogo di residenza del titolare del trattamento e dell'interessato, purché in Italia venga svolta qualunque operazione riconducibile alla nozione di trattamento.

Nel corso di questo capitolo verranno dunque approfondite suddette fattispecie, fornendo, ove possibile, casi pratici pervenuti, in ultima analisi, alla Corte di Cassazione, come il recentissimo caso *Vividown*[7]. Gran parte della trattazione sarà incentrata attorno al delitto del trattamento illecito di dati, reato che, per vari motivi, ha dato vita a molteplici pronunce e posizioni dottrinali non sempre concordanti, spostandoci poi sugli ulteriori reati che, come si è detto alla fine del II Capitolo, pongono interessanti profili problematici in tema di principio di offensività, per quanto riguarda il fenomeno della tutela di funzioni.

[7] La Corte di Cassazione, III Sez. Pen., si è pronunciata con sentenza n. 5107 del 3 febbraio 2014, ribadendo la posizione della Corte d'Appello di Milano, rigettando il ricorso del Procuratore Generale, circa un eventuale profilo oggettivo di responsabilità di un Internet Host Provider, nel caso di specie Google, in seguito ad un video offensivo caricato sulla piattaforma sociale Google Video nei confronti di un ragazzo affetto da sindrome di Down.

1.1 Trattamento illecito di dati: premessa (art. 167)

Il trattamento illecito di dati[8] è senza dubbio il reato del presente Codice che maggiormente stimola l'interprete e lo studioso del diritto penale per la sua ampia formulazione normativa e l'enorme casistica giurisprudenziale che porta in grembo. Per questo motivo, la sua trattazione deve essere necessariamente frazionata così da lasciare al lettore lo spazio necessario per apprendere, volta per volta, gli aspetti salienti della fattispecie, senza risultare eccessivamente caotica. In un primo momento risulterà necessario soffermarsi sulla disciplina del medesimo Codice richiamata dall'articolo 167 che, se violata, assieme agli ulteriori requisiti presenti nella fattispecie, perfeziona il delitto, e sui suoi conseguenti rilievi critici, intrinsecamente connaturati a questa tecnica del rinvio. In seguito, sarà analizzato il concetto di "trattamento" e la *ratio* del reato in questione, riprendendo alcuni temi già trattati in materia di bene giuridico tutelato. In ultima analisi, risolti i problemi scaturenti dal richiamo ai rami extrapenali del diritto, sarà approfondito il fatto tipico del reato, focalizzandosi su alcuni aspetti quali la nozione di "nocumento", più volte oggetto di pronunce da parte della Suprema Corte di Cassazione[9].

Per quanto concerne la sua struttura, tale fattispecie prevede una clausola di riserva, l'elemento oggettivo della violazione della normativa richiamata ed il trattamento illecito dei dati, accompagnato dal nocumento e, per quanto concerne l'elemento soggettivo, il dolo specifico.

---

[8] Trattamento illecito di dati (Art. 167): 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

[9] Fra le quali la ss. n. 30134 del 9 luglio 2004, III Sez. Pen. e la ss. n. 23798 del 15 giugno 2012, III Sez. Pen.

1.1.1 La violazione della normativa richiamata e le sue criticità

La violazione della normativa che l'articolo in questione richiama è differente a seconda che ci si riferisca al primo comma oppure al secondo comma della fattispecie. Cominciando dal primo comma, caratterizzato da sanzioni e, dunque, da ipotesi meno gravi, il trattamento illecito dei dati deve venire in violazione degli articoli seguenti.

La normativa extrapenale del comma I

Gli artt. 18 e 19, i quali stabiliscono i principi applicabili ai trattamenti compiuti da soggetti pubblici, esclusi gli enti pubblici economici, prevedono che il trattamento consentito è *soltanto* quello "*per lo svolgimento delle funzioni istituzionali*" e che non è richiesto il consenso dell'interessato[10]; inoltre per quanto riguarda i cd. dati comuni[11], il trattamento è consentito anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente. Per la comunicazione, invece, che richiede espressamente una norma di legge o un regolamento, è previsto che, se ha come destinatario un altro soggetto pubblico, è consentita *anche* quando sia "*necessaria per lo svolgimento di funzioni istituzionali*[12]".

L'art. 23 riguarda invece le regole del trattamento compiuto da privati ed enti pubblici economici i quali debbono sempre richiedere ed ottenere il consenso espresso dell'interessato, che dovrà pervenire per iscritto qualora il trattamento riguardi dati sensibili. Inoltre è stabilito che il consenso potrà ritenersi validamente prestato solo se *"è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per*

[10] Sono tuttavia esclusi, e dunque è necessario ricevere il consenso, gli esercenti le professioni sanitarie e gli organismi sanitari pubblici.

[11] Si ritengono tali quei dati diversi dai dati sensibili e giudiziari, che ex. art. 4 del presente codice, rispettivamente alle lettere *d* ed *e*, sono definiti come *"i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;"* e " *dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;*".

[12] Essa dovrà tuttavia rispettare un obbligo di preavviso di almeno 45 giorni al Garante, salvo sua diversa determinazione.

iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13[13]*"*. Di seguito però, l'articolo 24 prevede tutta una serie di casi[14] per i quali non è richiesto il consenso ai fini del trattamento, andando a restringere poi il principio applicativo dell'articolo 23.

Gli artt. 123, 126, 129 e 130 dettano la disciplina del trattamento dei dati relativamente alla "*fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni*". L'articolo 123 prevede, per quanto riguarda i dati relativi al "*traffico*", le condizioni specifiche che ne consentono il trattamento, la durata della loro conservazione ed il contenuto del'informativa che deve essere esibito all'abbonato o all'utente. L'articolo 126 impone invece l'anonimato sui dati relativi all'ubicazione diversi dai dati relativi al traffico. L'articolo 129 disciplina le modalità di inserimento e di utilizzo dei dati relativi agli abbonati in elenchi cartacei o telefonici a disposizione del pubblico[15]. Infine l'articolo 130 vieta le cd. comunicazioni indesiderate [16] in mancanza di consenso da parte dell'interessato, sancendo poi l'obbligo al mittente di fornire la sua identità reale o un idoneo recapito.

La normativa extrapenale del comma II

Venendo ora alla più grave ipotesi del secondo comma, il trattamento illecito deve avvenire in violazione dei seguenti articoli.

Il primo riferimento è all'articolo 17, relativo al trattamento di dati diversi da quelli sensibili e giudiziari, che presenta *"rischi specifici per i diritti e le*

[13] Quest'articolo tratta della "informativa privacy", requisito essenziale per cui gli interessati devono essere informati del fatto che un ente tratti i loro dati personali per determinati scopi e finalità e, laddove richiesto dalla legge, devono poter esprimere il loro consenso informato ovvero libero, espresso e consapevole, inoltre devono essere resi edotti dei loro diritti e di come devono fare per esercitarli, ai sensi dell'art. 7 (richiesta di informazione sui propri dati, aggiornamento o rettifica dei dati, cancellazione dei dati, opposizione al trattamento).

[14] Tra i più importanti casi in cui il consenso non è richiesto si ricorda la lettera a) adempimento di un obbligo previsto dalla legge o da un regolamento o una normativa comunitaria; b) se è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato.

[15] Subordinate, queste, all'osservanza di un provvedimento del Garante in cooperazione con l'Autorità per le garanzie nelle comunicazioni e in conformità alla normativa comunitaria.

[16] Quali spam, junk mail, abuso di messaggi pubblicitari per via telefonica, e così via. Sono definite come "*l'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitari o odi vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale"*.

libertà fondamentali, nonché per la dignità dell'interessato in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare". Successivamente è detto che il compito di riconoscere misure e accorgimenti di questo tipo è affidato al Garante in applicazione dei principi sanciti nel presente Codice.

In seguito sono richiamati gli artt. 20, 21, 22, comma 8° e comma 11° concernenti il trattamento dei dati sensibili e dei dati giudiziari da parte di soggetti pubblici. Essi sono consentiti solo se autorizzati da "*espressa disposizione di legge o provvedimento del Garante*" fermo restando il divieto di diffondere dati idonei a rivelare lo stato di salute dell'interessato e ammettendo invece, se previsti da espressa disposizione di legge, le operazioni di raffronto fra dati sensibili e giudiziari.

L'articolo 25 concerne invece il divieto di comunicazione e diffusione oltre[17] che nei casi disposti dal Garante o dall'autorità giudiziaria.

Gli artt. 26 e 27 disciplinano il trattamento dei dati sensibili e dei dati giudiziari da parte di soggetti privati. I primi possono essere oggetto di trattamento solo col consenso scritto dell'interessato e previa autorizzazione del Garante, per quanto riguarda i secondi, il trattamento da parte di privati o enti pubblici economici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante.

L'articolo 45, infine, impone il divieto di trasferimento anche temporaneo, al di fuori dei casi previsti dagli artt. 43 e 44, di dati personali verso un Paese non facente parte dell'Unione Europea *"quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato"*.

[17] È in riferimento ai dati personali sui quali è stata ordinata la cancellazione oppure è decorso il periodo di tempo previsto ex. art. 11, I comma, lettera *e,* e per le finalità diverse da quelle indicate all'interno del trattamento previsto, facendo poi salve le comunicazioni o diffusioni di dati richiesti, in conformità alla legge, dalle forze di polizia, autorità giudiziaria, organismi di informazione e sicurezza, per finalità di difesa e sicurezza dello Stato o di prevenzione, accertamento e repressione di reati.

Profili critici conseguenti alla tecnica del rinvio

Venendo ora agli aspetti più controversi che questa tecnica del rinvio porta con sé, preme rilevare come immediatamente, ad un primo colpo d'occhio, la sola lettura della fattispecie renda arduo il lavoro dell'interprete al fine di tratteggiare i contorni di questo delitto, dal momento che, volta per volta, "*è necessario individuare il cuore della norma di disciplina la cui violazione assurge a elemento essenziale del fatto di reato di trattamento illecito di dati ovverosia a selezionare nell'ambito di quelle norme di disciplina, gli aspetti più pregnanti la cui inosservanza si appalesi davvero significativa sul versante penalistico"*[18]. L'articolo 23, per esempio, prevede che il consenso sia valido se documentato per iscritto, tuttavia risulta evidente come l'eventuale inosservanza di quest'aspetto normativo non inficerebbe l'effettiva liceità del trattamento qualora permanessero altri requisiti sostanziali come la pienezza e consapevolezza dello stesso consenso. È evidente, dunque, come in questo caso non sempre sia facile tratteggiare in modo limpido la linea di divaricazione fra lecito e illecito penale, soprattutto per quanto riguarda i destinatari del precetto che, a differenza dell'interprete, non posseggono in linea di massima i requisiti per districarsi all'interno di una normativa così altamente articolata. Ulteriori dubbi relativi alla disciplina richiamata residuano in tema del già citato articolo 130. Ci si chiede come sia possibile ricondurre un caso di questo tipo alla *eadem ratio* rinvenibile all'interno degli altri richiami, dato che in questo caso il dato personale violato sarebbe al massimo il numero di telefono o l'indirizzo mail, e dunque non si capisce *"perché si è stabilito di presidiare con la sanzione penale tale condotta ed escludere per di più il caso di messaggi pubblicitari effettuati tramite personale della ditta. Spesso non meno subdoli ed invadenti dei primi"*[19].

Rimane altresì inspiegato l'utilizzo della più grave sanzione al comma 2° in caso di violazione dell'articolo 45 sul Trasferimento all'estero che, all'articolo

[18] DEL CORSO S., *La protezione dei dati personali,* a cura di BIANCA C. M., BUSNELLI F. D., CEDAM, 2007, Padova, pag. 2059 e ss.

[19] LUCENTE C., *La nuova normativa penale a tutela dei dati personali,* in CARDARELLI-SICA-ZENO ZENOCOVICH, *Il codice dei dati personali. Temi e problemi,* Milano, 2004, pag. 638 e ss.

37 della previgente disciplina, era invece punito col meno grave disposto del I comma.

Infine, permane il problema, forse più grave per il penalista, dei casi in cui è l'inosservanza di regole dettate in un provvedimento del Garante a dar vita all'illiceità del trattamento, configurando ipotesi di vere e proprie norme penali in bianco[20], con la inevitabile conseguenza di enucleare contenuti precettivi desumibili solo in fonti secondarie dalle quali si potrà poi ricavare la regola di condotta per il caso concreto. Ciò avviene quando è richiamata la violazione dell'articolo 129[21], oppure quella dell'articolo 17[22].

[20] Per norma penale in bianco si intende quella norma che rinvia ad un ramo extrapenale dell'ordinamento per la definizione di alcuni aspetti del precetto che risulta quindi essere determinato da norma diversa da quella che indica la pena. Sebbene in certi casi il rinvio non solo è doveroso, ma anche utile, in generale l'utilizzo della norma penale in bianco è stato criticato in quanto passibile di tracciare forti profili di indeterminatezza in seno alle fattispecie penali e, soprattutto, di minare in modo significativo il principio di legalità ex. art. 25 Cost. In questo modo, dovendo le singole regole di condotta e le sanzioni penali avere caratteri di generalità ed astrattezza, il principio di legalità impone anche una riserva di legge che descrive il monopolio del Parlamento nazionale sulla formazione della legge penale. In linea generale, come previsto dalla prima sentenza di Corte di Costituzionale su questo tema, n. 26 del 1966, il rinvio è da considerarsi non lesivo dei suddetti principi qualora integri il precetto solo con riferimento a contenuti di natura tecnica. In altre parole "*quando la legge fissi i presupposti, i contenuti, i caratteri e i limiti del reato, lasciando alla fonte subordinata soltanto una specificazione ma nell'ambito di una cornice già compiutamente delineata dal legislatore quanto alla valutazione della offensività del fatto e quindi alla meritevolezza della pena."* ANTOLISEI F., *Manuale di Diritto Penale – Parte generale,* Milano, Giuffrè Editore, 2003, pag. 56-57.

[21] Relativo alle modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi cartacei o elettronici a disposizione del pubblico, individuate con provvedimento del Garante.

[22] In cui è previsto che il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, prescritti tramite provvedimento del Garante.

1.1.2 Nozione del termine «trattamento», condotta e ratio della tutela

Definizione normativa di trattamento

Un grande sforzo esegetico è richiesto da parte dell'interprete anche in relazione alle problematiche che scaturiscono all'interno della fattispecie in questione, come per l'individuazione della condotta di trattamento. Di per sé, a prima vista, la nozione è immediatamente delineabile, poiché ai sensi dell'articolo 4, comma 1°, lett. a) si intende per trattamento "*qualunque operazione o complesso di operazioni , effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto , l'utilizzo,l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati"*. Rispetto a quanto previsto dalla L. 675/96 per il medesimo sostantivo, è stata inserita una nuova operazione di trattamento, la consultazione, aggiungendo inoltre che non occorre che, perché si abbia il trattamento, i dati siano registrati in una banca dati[23].

Come si vede, la definizione normativa di trattamento non sembra lasciare spazio ad eventuali dubbi; tuttavia, traslandola su di un piano prettamente penalistico, le cose tendono a complicarsi. Ciò che subito dovrebbe far riflettere l'interprete sarebbe il poter rintracciare, in una tale nozione di trattamento, anche per una soltanto delle operazioni descritte, una "*inammissibile estensione dell'orbita operativa della fattispecie penale"*. La posizione proposta in dottrina[24] è stata infatti quella di interpretare, in mancanza di una chiara posizione legislativa, la nozione penale di trattamento in forma autonoma rispetto a quella normativa. In questo modo si andrebbero a considerare come penalmente irrilevanti quelle operazioni, di per sé

[23] Né che siano in *"un qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti"* come previsto dall'articolo 4, comma 1°, lettera *p*.
[24] CORRIAS LUCENTE, *La nuova normativa penale a tutela dei dati personali,* in CARDARELLI-SICA-ZENO ZENOCOVICH, *Il codice dei dati personali. Temi e problemi,* Milano, 2004, pag. 635.

rientranti nella definizione di trattamento, da sole inidonee a produrre almeno una potenziale lesione del bene giuridico tutelato. Così, ritiene medesima dottrina, si andrebbe a valorizzare anche il plurale di "dati" come oggetto dell'illecito trattamento in quanto, stando alle pronunce di merito successive al presente Codice, il trattamento (spesso raccolta e diffusione) di un solo dato personale, estraneo ad una attività illecita di registrazione, "*elaborazione e fissazione di basi di dati (archivi o database) illegittimamente trattati, non integrerebbe la condotta tipica del precetto penale*[25]".

Tuttavia, preoccupazioni di questo tipo non sembrano essere, in fondo, condivisibili.

L'interpretazione dottrinale sul trattamento: un'estensione

Altra dottrina[26] ritiene infatti che la fattispecie in questione non tuteli in via primaria o anche solo concorrente il bene della riservatezza. A giustificazione di ciò è richiamata una sentenza della Cassazione civile[27], chiamata a risolvere un contrasto fra il Garante ed un Giudice di merito. Il principio di diritto da essa enunciato prevedeva che "*l'inesatto trattamento di dati personali legittima l'interessato ad invocare, presso la competente autorità di garanzia, la tutela di cui agli art. 1 ss*[28]*, a prescindere dalla circostanza che il dato personale inesattamente riportato sia soltanto diffuso nell'esercizio di attività giornalistica (e per tanto non sia destinato in tal caso ad alcuna "archiviazione"). La legge difatti, pur riservando particolare rilievo ai dati personali che presuppongano un'attività di archiviazione in banche dati, è purtuttavia funzionale, nelle sue linee generali, alla difesa della persona e dei suoi fondamentali diritti, che possono ben essere lesi dal trattamento anche*

[25] LUCENTE C., *La nuova normativa penale a tutela dei dati personali,* in CARDARELLI-SICA-ZENO ZENOCOVICH, *Il codice dei dati personali. Temi e problemi,* Milano, 2004, pag. 636.
[26] DEL CORSO S., *La protezione dei dati personali,* a cura di BIANCA C. M., BUSNELLI F. D., CEDAM, 2007, Padova, pag. 2061-2064.
[27] Cass. civ., sez. I, 30 giugno 2001, n. 8889. Una persona, dopo aver chiesto inutilmente e reiteratamente al direttore di un quotidiano nazionale di rettificare un suo dato personale riportato in modo inesatto, aveva fatto richiesta di rettifica direttamente al Garante, che fu poi accolta. In sede di opposizione però, il Tribunale aveva riformato tale provvedimento sull'assunto che la L. 675/96 tutelasse il trattamento dei dati solo in riferimento alla loro archiviazione.
[28] Che in quel caso, ovviamente, erano ancora quelli della L. 675/96.

solo giornalistico dei dati, in considerazione della loro sola diffusione ed a prescindere dalla conseguente strutturazione in archivio."

Di conseguenza si è ritenuto applicabile tale principio anche al presente Codice che, all'articolo 1, prevede che chiunque ha diritto alla protezione dei dati personali che lo riguardano. In linea con questa posizione dottrinale si è ritenuto che, anche ai sensi di codesto articolo, si debba riconoscere non una protezione assoluta ed intransigente della privacy, bensì una protezione, espressone di un modello "relazionale", di diversi valori che il riferimento alla privacy necessariamente sottintende ma che poi si bilancia con ulteriori valori di rango costituzionale, così da dar vita ad un bilanciamento di interessi tendenzialmente configgenti[29]. Alla luce di ciò si ritiene non essere stata volontà del legislatore incriminare il trattamento illecito di dati semplicemente come a tutela assoluta del diritto alla riservatezza, avendolo invece inteso piuttosto come a tutela di un diritto all'esclusivo controllo dei dati della propria vita, riallargando il concetto di riservatezza oltre i suoi iniziali confini.

Ecco quindi che, sulle linee guida di questo approccio dottrinale, ben si posa una definizione del Mantovani sul concetto di riservatezza, inteso come diritto che può essere definito come il "*diritto alla esclusività di coscienza di tutto ciò che attiene alla propria vita privata"* il quale, se conosciuto o rivelato, potrebbe arrecare nocumento *"al sottostante interesse alla "privatezza", bisogno essenziale della persona umana"*[30].

Tuttavia, come si è accennato, né la vecchia legge sulla privacy, né l'attuale Codice, sembrerebbero tutelare quest' aspetto più pregnante del diritto alla riservatezza, focalizzandosi piuttosto sulla disciplina del trattamento di dati personali, pubblici o privati. Di conseguenza, non sembra potersi prescindere, nel definire la nozione di trattamento, dalla dimensione teleologica che rafforza le operazioni di cui esso stesso è composto, vale a dire quelle

[29] Questa la posizione di BUSNELLI F. D., *Dalla legge al codice: un dilemma, una sfida, un consolidamento normativa, una (imperfetta) razionalizzazione delle tutele,* in *La protezione dei dati personali,* a cura di BIANCA C. M., BUSNELLI F. D., CEDAM, 2007, Padova, cap. XXXV.

[30] MANTOVANI F., *Diritto penale. Parte speciale I. Delitti contro la persona,* Padova, 1995, pag. 473-475

operazioni che, per assumere rilievo all'interno del Codice, debbono necessariamente rientrare nell'ambito di un'attività di organizzazione, e quindi di archiviazione, di un insieme di dati personali.

A seguito di ciò, potrebbe concludersi che, accogliendo questa posizione dottrinale, la fattispecie in esame sia fortemente in grado di tutelare la porzione positiva del concetto di riservatezza, sul quale ci siamo dilungati nel capitolo precedente, ma fatichi invece ad apportare chiare porzioni di tutela nei confronti di quella fetta negativa del diritto alla riservatezza, nucleo antico ed inossidabile dal quale ogni argomento in questione è cominciato. Personalmente, qualora si accettasse una posizione di questo tipo, non si farebbe tuttavia fatica a ricercare, all'interno dell'ordinamento, ulteriori fattispecie che tutelino in maniera soddisfacente quest'aspetto negativo della privacy, e sulle quali presto ci soffermeremo affrontando i reati privacy impropri.

La rivalutazione sul bene giuridico tutelato

Di conseguenza, volendo tracciare la *ratio* di tutela che il trattamento illecito di dati offre e, dunque, anche il bene giuridico tutelato, può valere quanto segue. Partendo dal fatto che, indubbiamente, tale reato tuteli, quantomeno positivamente, il diritto alla riservatezza, si potrebbe aggiungere che esso non sia l'unico bene oggetto di tutela[31]. In effetti, sebbene subordinare la punibilità al nocumento evidenzi la volontà del legislatore di porre rilievo sul diritto individuale dell'interessato, non si può per ciò solo escludere che la norma tuteli anche le mere funzioni, vale a dire, le funzioni di controllo del Garante per la protezione dei dati personali. Si potrebbe quindi parlare di reato plurioffensivo[32], possibilità confermata almeno in parte dal fatto che il reato è

[31] VILLANI C., *Il codice del trattamento dei dati personali,* a cura di CUFFARO-D'ORAZIO-RICCIUTO, Giappichelli, 2006, Torino, pag. 743.

[32] Molto esaustivi sul tema VENEZIANI P., *Beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali,* tratto da *Il diritto penale dell'informatica nell'epoca di internet,* a cura di L. Picotti, Padova, 2004, pag. 166 e MANNA A., *Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali,* in *Il diritto dell'informazione e dell'informatica,* 2003, n. 4-5, pag. 730 i quali ritengono come una corretta politica criminale ispirata al principio di sussidiarietà avrebbe dovuto evidenziare la natura fortemente personale di tale diritto nonché disponibile, sfruttando la procedibilità a querela. Il mantenimento della

procedibile d'ufficio e non a querela, come più frequentemente accade se l'oggetto della tutela fosse singolo e a protezione del solo diritto alla riservatezza.

Una considerazione finale sul bene giuridico tutelato, anche alla luce delle posizioni dottrinali riportate, si può sviluppare attorno alla clausola di riserva "*salvo che il fatto costituisca più grave reato"*. Come è ovvio, ciò denota la natura di reato sussidiario che viene assorbito qualora il fatto possa egualmente rientrare all'interno di un'ulteriore previsione penale che la contenga e appaia inoltre più grave. Tuttavia, nel caso in cui il trattamento di dati appaia essere funzionale ad una condotta più grave, ne andrebbe a costituire parte integrante, nonché presupposto logico e fattuale[33], fondendo di conseguenza il bene giuridico dell'articolo 167 del Codice all'interno di quello della fattispecie più grave, riprendendo così quelle correnti dottrinali di cui *supra,* per le quali necessariamente il trattamento illecito può, in certi casi, espandere la sua area protettiva al di fuori della sua stessa portata.

---

procedibilità d'ufficio conferma pertanto la natura *"anfibia"* di quest'illecito, a metà fra la tutela di funzioni e la protezione di un bene giuridico individuale.

[33] Così ritiene CORASANITI G., *Sanzioni penali e depenalizzazione degli illeciti nella normativa a tutela dei dati personali,* in *Danno e responsabilità,* 2002, pag. 698 e ss. ma anche PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali,* Milano, 2003, pag. 516.

1.1.3 Ulteriori elementi strutturali del reato e clausola di riserva

Le ulteriori condotte: comunicazione e diffusione

Alla luce di quanto detto, è ora possibile addentrarsi nelle condotte incriminate dall'articolo 167 del presente Codice. Il legislatore vieta il trattamento che avvenga in violazione delle norme disciplinari sopra richiamate, prevedendo, al comma 1°, seconda parte, una sanzione leggermente più grave nel caso in cui il fatto consista nella "comunicazione" o "diffusione", ed invece una sanzione lievemente meno grave, nella prima parte del comma 1°, se dal fatto (il trattamento) derivi nocumento.

Partendo dal primo, le definizioni di comunicazione e diffusione sono rinvenibili all'articolo 4, comma 1°, lettere *l)*[34] ed *m)*[35]. Nel comma 2°, invece, la distinzione fra comunicazione e diffusione da un lato e trattamento dall'altra, non è evidenziata, mantenendo un'unica sanzione, la più grave della fattispecie; ciò è essenzialmente dovuto alla specificità del trattamento nei casi previsti dal comma 2°, nonché dal fatto che la disciplina richiamata ha spesso ad oggetto proprio un divieto di comunicazione o diffusione. L'equiparazione sanzionatoria di due condotte così diverse è, per alcuni[36], indice di una violazione del principio di ragionevolezza e dunque incostituzionalità della norma.

Inoltre, fra queste due condotte e quella del trattamento dal quale derivi nocumento è aperto il dibattito in tema di circostanza aggravante o titolo autonomo di reato. Se si optasse per la natura di mera circostanza aggravante, si andrebbe anche ad affermare che la punibilità di comunicazione o diffusione sia condizionata dalla presenza di un effettivo nocumento verso l'interessato,

---

[34] *"Dare conoscenza ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma ,anche mediante la loro messa a disposizione o consultazione"*.

[35] "*Dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione"*.

[36] VILLANI C., *Il codice del trattamento dei dati personali,* a cura di CUFFARO-D'ORAZIO-RICCIUTO, Giappichelli, 2006, Torino, pag. 746. Per l'Autore, non essendo dubitabile che la diffusione di dati sia una condotta di gran lunga più grave rispetto alla comunicazione, dal momento che i destinatari della prima sono una pluralità indeterminata e non un singolo o più soggetti determinati come nella comunicazione, risulta inverosimile che le due differenti aggressioni allo stesso bene giuridico, siano tuttavia punite con la medesima pena.

dando vita ad una forzatura normativa lampante, dal momento che il riferimento al nocumento è chiaramente rapportato al solo primo periodo del comma 1° relativo al trattamento, non anche al secondo. Per questo pare corretto ritenere che relativamente alle condotte di comunicazione e diffusione, ci si trovi di fronte ad una fattispecie autonoma di reato[37]. Di conseguenza la norma sarebbe caratterizzata da due sotto-fattispecie autonome: il trattamento illecito dal quale derivi nocumento ed il trattamento illecito di dati mediante comunicazione o diffusione[38].

Il dolo specifico

Prima di affrontare la tematica relativa al nocumento, bisogna a ciò premettere che, affinché la fattispecie si perfezioni, sia soddisfatto il dolo specifico[39] [40] di trarre per sé o per altri profitto o (alternativo) di recare ad altri un danno. Sul punto, si è talvolta proposta una interpretazione di profitto in chiave non necessariamente patrimoniale, così che possa valere come sinonimo di vantaggio, allargando conseguentemente i casi in cui il trattamento comporterà al soggetto agente una qualche utilità; alla stessa si è opposta la posizione per la quale, mantenendo l'accezione patrimonialsita del dolo specifico, la disposizione in esame si applicherebbe nelle sole eventualità in cui il titolare abbia effettuato un trattamento illecito per conseguire una qualche utilità economica o per produrre un intenzionale danno patrimoniale ad altri. Dunque, la funzione selettiva di limite alla punibilità all'articolo 167, sembra essere maggiormente quella svolta dal requisito del nocumento arrecato

[37] Infatti manca anche qualsiasi rapporto di *genus* a *species* rispetto all'ipotesi contemplata dal primo periodo del comma 1°.

[38] Quindi quest'ultima si porrebbe in rapporto di progressione criminosa rispetto alla prima e all'interesse tutelato, in quanto la condotta di trattamento con comunicazione o diffusione ha un grado di offensività maggiore di quella del trattamento di cui primo periodo, comma 1°.

[39] Si ricorda che ci si riferisce al dolo generico, nozione tipica del dolo, quando la fattispecie richiede che il soggetto agente agisca con coscienza e volontà di tutti gli elementi tipici della fattispecie, così che vi sia completa corrispondenza fra ideazione e realizzazione. Il dolo specifico, richiede inoltre, inglobando all'interno di sé il dolo generico, che il soggetto agisca anche per una'ulteriore finalità al di fuori di tutti gli elementi del fatto tipico, tuttavia, perché il reato si perfezioni, non è richiesto che quella ulteriore finalità effettivamente si verifichi, essendo sufficiente la volontà di perseguirla. ANTOLISEI F., *Manuale di Diritto Penale – Parte generale,* Milano, Giuffrè Editore, 2003, pag. 345 e ss.

[40] Secondo parte della dottrina, la qualificazione del dolo in termini di intenzionalità specifica mirerebbe ad evitare il ricorso da parte del giudice, nell'ambito del giudizio di colpevolezza, al dolo eventuale: IMPERIALI R., *Codice della Privacy,* Il sole 24 ore Pirola, Firenze, 2004, pag. 695.

all'interessato dal trattamento, lasciando così più ampia applicazione al termine profitto[41].

Il concetto del nocumento al vaglio della Corte di Cassazione

Venendo ora all'aspetto forse più controverso della fattispecie, vale a dire il nocumento, è necessario ricordare che la vecchia formulazione dell'illecito della L. 675/96 lo prevedeva solamente come circostanza aggravante di fronte ad un cospicuo aumento di pena. Oggi, invece, esso non costituisce più circostanza aggravante, venendo bensì utilizzato in entrambe le due ipotesi del trattamento in qualità, almeno in prima analisi, di elemento costitutivo. In questo modo si è abbandonata quella posizione di "delitto aggravato dall'evento"[42] che ritraeva la fattispecie antecedente quale di pericolo presunto (o astratto)[43] passando invece ad un reato maggiormente aderente al principio di offensività sancito in Costituzione, vale a dire di pericolo concreto. Circa il significato del termine, può dirsi che con nocumento può intendersi "*un qualsiasi reale pregiudizio, giuridicamente rilevante, patrimoniale o non patrimoniale*" [44]. In seguito però, molto si è dibattuto, subito dopo l'emanazione del Codice Privacy, sulla concreta applicabilità del nocumento, come riformulato dal nuovo articolo 167. Importante qui, la sentenza di Cassazione del 28 maggio 2004 n. 30134[45]. È la stessa Corte che, *in primis,* riconosce come, nel nuovo reato di trattamento illecito di dati, si sia passati da

[41] Su questa linea di principio è anche conforme la Cassazione che in sentenza n. 30134 del 9 luglio 2004, III Sez. Pen., ritiene come i termini di profitto e danno devono essere intesi nella loro massima estensione, comprendendo tutte le situazioni di pregiudizio e vantaggio, anche non patrimoniale.

[42] Si diceva, infatti, che l'aggravante del nocumento dovesse ritenersi sempre presente, come una sorta di aggravante *in re ipsa*, a meno di non "*interpretare lo stesso nocumento come un danno diverso ed ulteriore rispetto a quello insito nel fatto stesso della divulgazione* contra legem *del dato personale*". Così VENEZIANI P. *Beni giuridici protetti e tecniche di tutela penale,*in *Rivista trimestrale di diritto penale dell'economia,* 1997, pag. 144.

[43] Come riteneva LUCENTE C., *Sanzioni penali e amministrative a tutto campo per aumentare la tutela del cittadino,* in *Guida al diritto,* 1997, n. 4, pag. 82.

[44] Secondo la pacifica posizione di MANTOVANI F., *Diritto penale. Parte speciale I. Delitti contro la persona,* Padova, 1995, pag. 513.

[45] La Corte fu chiamata a decidere se la trattazione dei dati personali degli appartenenti ad un'associazione umanitaria, derivanti da un elenco riservato, e utilizzati senza consenso da parte di un componente dell'associazione, per l'invio di materiale di propaganda elettorale per la propria candidatura a consigliere comunale, potesse integrare il nuovo reato in esame. Di cui molto è stato affrontato in SICA S., *"Danno" e "nocumento" nell'illecito trattamento di dati personali,* in *Il diritto dell'informazione e dell'informatica,* 2004, n.4-5, pp. 715-727 e in ANTONINI E., *Il trattamento illecito di dati personali nel codice della privacy: i nuovi confini della tutela penale,* in *Diritto penale e processo,* 2005, n. 3, pp. 338-346.

una fattispecie di pericolo presunto (o astratto) ad una di pericolo concreto, così che anche i termini di profitto e danno risulterebbero maggiormente tipicizzati; per chiarire ciò la Corte, facendo luce sul concetto di nocumento, si pone innanzitutto il problema di ricostruire la natura giuridica della previsione[46], quale condizione obiettiva di punibilità o elemento costitutivo della fattispecie[47]. La Corte sceglie la via della condizione obiettiva di punibilità intrinseca[48]: se infatti si ritenesse che il nocumento fosse elemento costitutivo del reato, allora lo stesso dovrebbe necessariamente rientrare nel fuoco del dolo della fattispecie; di conseguenza si avrebbe quale evento del reato il fine perseguito dal soggetto agente che, in quanto riconducibile allo schema del dolo specifico, non deve necessariamente realizzarsi ai fini della consumazione del reato. Inoltre, da un punto di vista squisitamente letterale, si è aggiunto che l'espressione utilizzata dal legislatore non è conforme al classico *"se il fatto cagiona"*[49], solitamente usato per configurare un elemento costitutivo della fattispecie quale evento del reato.[50]

In seguito, toccando il significato del termine nocumento, la Corte ritiene che *"questo concetto […] sembra maggiormente tipizzare un evento di danno direttamente ed immediatamente collegabile e documentabile nei confronti dei soggetti cui i dati raccolti sono riferiti, sicché deve aversi riguardo ad ipotesi concrete di* vulnus *e di discriminazioni a causa dell'intervenuta violazione della normativa richiamata nel precetto penale"*. Così la Corte ha inteso

[46] "*Se dal fatto deriva nocumento".*

[47] Si ricorda che con condizione obiettiva di punibilità si intende un avvenimento del mondo esteriore, futuro e incerto, estraneo alla condotta illecita, non necessariamente voluto dall'agente che di conseguenza risulta distinto dalla condotta criminosa e dall'evento tipico. Invece, qualora si parli di elemento costitutivo, ci si riferisce ad un elemento strutturale della fattispecie, che dunque rientrerà negli elementi richiesti all'interno del dolo in capo al soggetto agente.

[48] In dottrina, seppur non pacificamente, la condizione obiettiva di punibilità si distingue in intrinseca, cioè quella che aggrava l'implicita offesa insita nella commissione del reato, ed estrinseca, cioè quelle che non aggiungono alcuna lesione al bene protetto dalla fattispecie, essendo di natura politico-criminale. Fra i tanti si veda a riguardo MARINUCCI, DOLCINI, *Manuale di diritto penale, Milano*, 2012, pag. 377 e ss.

[49] La stessa considerazione viene fatta, ad esempio, seppur su in tema diverso, da PEDRAZZI C., *I reati fallimentari,* in PEDRAZZI e AA.VV., *Manuale di diritto penale dell'impresa,* Bologna, 1999, pag. 107.

[50] Come detto la dizione del reato in questione è stata usata anche per altri reati, si veda l'art. 612, comma 2° o gli artt. 423 e 580 c.p.

escludere le semplici violazioni formali ed irregolarità procedimentali, e tutte le inosservanze che producano un *vulnus* minimale all'identità personale e alla privacy del soggetto, tali da non determinare un apprezzabile danno nei suoi confronti. Dunque, nel caso di specie, adottando la Corte questa ragionevole posizione restrittiva, giunge a annullare senza rinvio la sentenza impugnata, perché l'imputato non è punibile ai sensi dell'articolo 167 D.lgs 196/2003.

La clausola di riserva

Resta da affrontare, in chiusura, il tema della clausola di riserva, che il legislatore recupera, nuovamente, dalla vecchia disciplina. Secondo lontana ma solida dottrina, si ritiene che la funzione delle clausole di riserva consista nell'impedire "*l'applicazione della norma che la contiene, quando, pur realizzandosi gli estremi di questa norma si realizzino anche quelli della disposizione cui la clausola rinvia*"[51]; il che significa che le clausole, per poter operare, presuppongono che si realizzi una particolare situazione giuridica in cui concorrano gli estremi di entrambe le norme collegate dalla riserva.

A partire dai lavori preparatori della legge del '96, si è ritenuto[52] che, con la clausola in questione, si sia voluto salvaguardare in particolare l'applicazione delle norme penali sull'abuso di ufficio e sulla rivelazione ed utilizzazione dei segreti d'ufficio (ex. artt. 323 e 326 c.p.). Tuttavia, per quanto concerne il rapporto fra l' articolo 167 del presente Codice e l'articolo 326 c.p., non ogni rivelazione o utilizzazione rientra nel concetto di "comunicazione", "diffusione" o "utilizzazione" del trattamento illecito di dati né tantomeno vi è sempre corrispondenza fra la nozione di dati personali e quella di notizie d'ufficio, quindi la clausola di riserva opererà solo quando il pubblico agente "comunichi" o "diffonda" o "utilizzi" nell'ambito di un trattamento di dati che siano coperti da segreto d'ufficio.

[51] DE FRANCESCO G. A., Lex specialis. *Specialità ed interferenza nel concorso di norme penali,* Milano, 1980, pag. 141.
[52] Così BUTTARELLI G., *Banche dati e tutela della riservatezza,* Milano, 1995, pag. 535.

Invece, in rapporto con l'abuso d'ufficio[53], il punto di intersezione sembra rinvenirsi nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, trattando dati personali in violazione del Codice Privacy che attengono al trattamento pubblico di questi, arrechi un nocumento all'interessato, al fine di trarne per sé o per altri un ingiusto vantaggio patrimoniale o di recare ad altri un danno ingiusto. Tuttavia, in ambedue i casi, la pena edittale prevista è identica nel massimo ma inferiore nel minimo a quella stabilita dal comma 2° dell'articolo 167 del presente Codice.

[53] *"E' punito il pubblico ufficiale o l'incaricato di pubblico servizio che, nello svolgimento delle funzioni o del servizio, in violazione di norme di legge o di regolamento, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto."*

1.1.4 Risvolti pratici all'interno dell'attuale realtà informatica: il caso Vividown e l'impatto sui social network

Uno degli ultimi temi da analizzare, volutamente lasciato alle conclusioni finali sul trattamento illecito per via di alcuni evidenti casi pratici seguenti, è quello relativo al soggetto attivo del reato.

Il soggetto attivo

La disposizione punisce semplicemente "chiunque"; di conseguenza, considerare tale fattispecie quale reato comune appare la soluzione più evidente. In effetti, questa è anche l'unica soluzione corretta, sebbene con le precisazioni che seguiranno; tuttavia non sono mancate, in passato, posizioni[54] che riconoscevano, come soggetto attivo del reato, solo il titolare del trattamento cioè "*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*" (art. 4, comma 1°, lett. f) del presente Codice). Tra l'altro, la stessa Suprema Corte[55] ha ribadito più volte la sua natura di reato comune, in quanto il divieto di diffusione di dati sensibili riguarda indistintamente tutti i soggetti entrati in possesso di dati, i quali saranno tenuti a rispettare sacralmente la privacy di altri soggetti entrati con i primi in contatto.

Tuttavia, sebbene sembri pacifica la natura di reato comune, ciò necessariamente non significa che la figura del titolare del trattamento non debba più essere presa in considerazione su questo tema, al contrario, soprattutto per quanto riguarda la sua configurabilità omissiva, tale figura torna ad assumere tutta la sua importanza quale fondamento di una eventuale posizione di garanzia[56] di natura formale. Un recentissimo caso[57], cd.

[54] Come fa notare TRONCONE P., *Il delitto di trattamento illecito di dati personali,* Giappichelli, Torino, 2011, pag. 91.
[55] Tra le più recenti si fa notare la sentenza n.21839 del 2011, III Sez. Pen.
[56] Si ricorda che per posizione di garanzia (come ricavabile ex. art. 40 c.p.) si intende quella situazione soggettiva in cui vertono determinati soggetti aventi un obbligo giuridico di impedire un evento, in

Il caso Vividown

"Vividown", aiuterà ad analizzare al meglio tale problematica: esso riguarda la diffusione da parte di una studentessa di un video, caricato sulla piattaforma "Google Video" contenente i dati personali e sensibili di un ragazzo disabile, ritratto mentre era oggetto di parole ingiuriose da parte di altri compagni di classe. Il Procuratore Generale ricorre in Cassazione ritenendo sussistente una responsabilità penale dei manager di Google, tramite l'asserita effettuazione di un trattamento di dati da parte di Google, in qualità di hosting provider[58] attivo. La Corte al contrario, non riconosce il ruolo di Google come trattamento precedentemente analizzato, non essendo quindi ad essa riconducibili gli obblighi propri del titolare[59]. L'host provider, infatti, ha una sua specifica disciplina contenuta nel D.lgs 70/2003 in materia di commercio elettronico per la quale, al ricorrere di determinate condizioni[60], ricopre una posizione di totale estraneità rispetto al materiale caricato dagli utenti, posizione che, evidentemente, non gli consente l'esercizio di alcun potere decisionale tale da condizionarne le modalità, i mezzi e gli scopi del trattamento dei dati personali e che, soprattutto, è anche estranea dalla figura

---

qualità di protettori del bene giuridico tutelato; in dottrina, la posizione di garanzia può avere legittimazione solo da fonti giuridiche formali (formalistica), oppure derivante da un esigenza solidaristica, con consequenziale creazione di un vincolo fra soggetto debole e garante del bene giuridico (sostanzialistica).

[57] Si tratta della sentenza di Cassazione n. 5107 del 3 febbraio 2014, Sez. III Pen., cd. Sentenza Vividown. Tale sentenza riconferma l'assoluzione della Corte d'Appello di Milano, a seguito della condanna rilevata in Primo Grado, di alcuni manager di Google, condannati proprio per trattamento illecito di dati personali. Le vicende processuali di cui si tratta scaturiscono dalla pubblicazione di un filmato sulla piattaforma *Google Video*, che ritrae un ragazzo disabile molestato ed insultato da alcuni compagni di scuola, i quali, inoltre, rivolgono pesanti offese anche all'indirizzo dell'associazione *Vivi Down.* Per tali fatti, i manager erano stati imputati per concorso omissivo nel delitto di diffamazione nei confronti del minore e dell'associazione (artt. 40, comma 2, e 595 c.p.), nonché per aver effettuato un illecito trattamento dei dati personali tramite un omissione di un informativa privacy visualizzabile in italiano dalla pagina iniziale del servizio, in sede di attivazione del relativo account, al fine di porre in essere l'upload di files.

[58] Con cui si intende un soggetto in grado di fornire ad utenti un servizio via internet di hosting, cioè di allocazione,tramite upload, di file, solitamente all'interno di un limite di spazio prestabilito. Il Procuratore ha ritenuto sussistente inoltre, a titolo di dolo specifico, il profitto derivante da una volontaria disattenzione sui contenuti del video, in modo tale da riuscire ad ottenere dalla sua permanenza in rete, anche solo eventualmente, un introito economico attraverso l'inserimento di *link* pubblicitari.

[59] Gli artt. 13, 17, 23 e 26 del Codice della privacy.

[60] Tale decreto, relativo al commercio elettronico, prevede che non vi sia responsabilità del provider per le condotte illecite tenute dagli utenti, se, ex. art. 16: *a)* non ne fosse effettivamente a conoscenza; *b)* una volta ricevuta la segnalazione dalle autorità competenti, si sia prontamente attivato per la rimozione dei contenuti illegittimi.

del titolare del trattamento del Codice Privacy. Nel dettaglio, sempre in riferimento alla normativa sul commercio elettronico di cui al D.lgs 70/2003, la Cassazione muove un'ulteriore critica all'impostazione accusatoria, circa la pretesa inapplicabilità del contenuto di tale decreto legislativo in materia di trattamento di dati personali. In realtà, evidenzia la Suprema Corte, le due disposizioni sono suscettibili di una lettura congiunta, in quanto il D.Lgs. 70/2003 costituisce, unitamente alla normativa sulla privacy, un quadro giuridico coerente e completo, venendo in rilievo nel caso in esame *"non in via diretta ma solo in via interpretativa, al fine di chiarire ulteriormente e confermare la portata che la disciplina in materia di privacy ha già di per sé"*. Tale concezione, per la Corte, non perde di coerenza logica nonostante la previsione di cui all'art. 1, comma 2°, lett. b, D.Lgs. 70/2003 richiamato dalla dal Procuratore Generale, che escluderebbe l'applicabilità delle disposizioni sul commercio elettronico alle questioni riguardanti proprio il diritto alla riservatezza ed in particolare il trattamento dei dati personali. La norma in questione, quindi, non avrebbe altra funzione se non quella di indicare che la tutela dei dati personali è disciplinata da un *corpus* normativo a sé stante (cioè il Codice della privacy), che rimane in ogni caso applicabile in ambito telematico anche dopo l'entrata in vigore della normativa sul commercio elettronico[61].

Tra le due discipline, dunque, sussiste un'armonia sul piano interpretativo ed applicativo *"perfettamente riscontrabile nel caso della determinazione dell'ambito di responsabilità penale dell'Internet host provider relativamente ai dati sensibili caricati dagli utenti sulla sua piattaforma"*. A conforto di quanto dedotto dalla Cassazione, si rileva che la definizione del concetto di titolare del trattamento dati fornita dal Codice della privacy, incentrandosi, come detto *supra*, sull'esistenza di un potere decisionale in ordine alle finalità,

[61] SALVI R., *La Corte di Cassazione sul caso Google vs Vivi Down: l'host provider non governa il mare magnum della rete,* in *Diritto civile e commerciale,* in *Diritto.it*, 2014, consultato il 16/07/14, http://www.diritto.it/docs/36069-la-corte-di-cassazione-sul-caso-google-vs-vivi-down-l-host-provider-non-governa-il-mare-magnum-della-rete?page=1

alle modalità ed agli strumenti del trattamento di dati personali, risulta perfettamente compatibile con le limitazioni di responsabilità previste dal D.Lgs. 70/2003. In effetti, il *provider* che non sia gravato da un generale dovere di sorveglianza, né sia a conoscenza della presenza di contenuti illeciti liberamente caricati da terzi sulla propria piattaforma, beneficiando in tal modo delle esclusioni previste dalla normativa sul commercio elettronico, non potrà in alcun modo compiere atti tali da esercitare un potere decisionale sul trattamento di dati personali relativi ai suddetti contenuti, restando estraneo agli stessi, e non rientrerà, pertanto, nella definizione normativa di "titolare" di cui all'art. 4, comma 1, lett. f.

Inoltre, sempre a supporto di ciò, la Corte fa notare come questa posizione sia anche in linea con la giurisprudenza comunitaria, evidenziando che *"l'esonero dalla responsabilità per i contenuti caricati si applichi al prestatore di un servizio online qualora non abbia svolto un ruolo attivo che gli permetta di avere conoscenza o controllo circa i dati memorizzati*"[62]. Dunque, come si evince, rimanendo semplicemente sul piano dell'elemento oggettivo, la Corte risolve tale questione districandosi abilmente fra le sottili differenze che possono nascere attorno al soggetto attivo di tale reato, dettando anche una soluzione convincente[63] nei casi in cui si debba rintracciare una posizione di garanzia per omissione derivante dal trattamento illecito di dati.

L'applicazione dell'illecito trattamento di dati nei social network:

Un conclusivo profilo d'interesse, da considerarsi assolutamente attuale, è quello concernente il trattamento illecito di dati derivante dall'utilizzo dei *social network*. Su questo tema nel quale, si vedrà, non molto è giuridicamente certo, la prima parte della questione si sviluppa, ulteriormente, attorno alla

[62] Così, Corte di Giustizia dell'unione Europea, sentenza del 12 luglio 2011, causa C-324/09 (L'Oreal SA / eBay), in Gazzetta Ufficiale dell'unione Europea del 10.09.2011.

[63] Circa le posizioni dottrinarie sviluppatesi nel corso degli episodi in questione si vedano: ALBAMONTE, *La responsabilità penale dell'internet provider: tra libertà di comunicazione e tutela dei singoli*, in *Questione giustizia*, 2010, 3, 184; BEDUSCHI, *Caso Google: libertà d'espressione in Internet e tutela penale dell'onore e della riservatezza,* in *Corr. Merito,* 2010; CASSANO, *Riflessioni a margine di un convegno sul caso Google/Vivi Down,* in *Riv. Pen.,* 2010; LOTIERZO, *Il caso Google – Vivi Down quale emblema del difficile rapporto degli internet* providers *con il codice della privacy,* in *Cass. pen.,* 2010, 11; MANNA, *La prima affermazione a livello giurisprudenziale della responsabilità penale dell'internet provider: spunti di riflessione tra diritto e tecnica,* in *Giur. Cost.,* 2010.

nozione di nocumento. Innanzitutto, una recente sentenza di Cassazione[64] sembra, infatti, aver nuovamente ritoccato tale concetto, ritenendo possibile un estensione del nocumento anche a terzi rispetto all'attività di trattamento. Considerando innanzitutto un nocumento *in re ipsa*, data la mole dei soggetti coinvolti, la Corte riconosce un effettivo ed ulteriore nocumento anche nei confronti della società costituitasi parte civile[65]. Francamente, una posizione di questo tipo risulta difficilmente condivisibile, come si è anche immediatamente rilevato in dottrina[66]: affermare l'esistenza di un nocumento penalmente rilevante, derivante da una responsabilità ex. art. 2050 c.c. significherebbe innanzitutto dar vita ad una probabilmente azzardata forzatura, considerando attività pericolosa l'illecito trattamento dei dati, ed inoltre scavalcherebbe completamente quella concezione sistematica propria del Codice Privacy, secondo il quale si tutelino i dati personali degli interessati e non per gli interessi commerciali di terzi. Ciò tuttavia potrebbe effettivamente complicare l'applicazione del trattamento illecito nei *social network*[67] in tutti quei casi in cui si debba provare in concreto il nocumento nei confronti di una gran quantità di utenti. Quest'aspetto riguarda, infatti, il lato prettamente

nei confronti di una pluralità di utenti…

[64] Sez. III, n. 23798, 15 giugno 2012. In estrema sintesi, la vicenda è relativa all'utilizzo da parte di una società dell'elenco di indirizzi di posta elettronica di iscritti ad un servizio di newsletter, gestito da altra società, con cui la prima aveva in passato sottoscritto un contratto di concessione di spazi pubblicitari; terminato il rapporto, continuava comunque l'utilizzazione di gran parte di quegli indirizzi (ben 177.090) con inoltro di newsletter senza il loro preventivo consenso.

[65] Ed a giustificazione di ciò, la Corte richiama un precedente in cui i giudici avevano affermato l'integrazione della condizione obiettiva di punibilità del nocumento nel danno morale sofferto dai parenti di una persona di cui erano state pubblicate le foto mentre era agonizzante poco prima di morire, ritenendo che nel'attività di trattamento fosse applicabile l'art. 2050 c.c., norma che si applica ai danti risentiti da chiunque in conseguenza di attività intrinsecamente pericolose verso la collettività (Sez. Civ. III, n. 24991/2011).

[66] LOTIERZO R., *Del nocumento nell'illecito trattamento dei dati personali ovvero dell'esigenza di ascendere alle origini di una incriminazione,* in *Cassazione penale,* 2013, n.4, pag. 1593.

[67] "*Il social network viene definito come una piattaforma di comunicazione online in grado di permettere all'utente la creazione di reti d'utenti che condividono i suoi stessi interessi, lo stesso deve essere inquadrato come servizio della società dell'informazione, ai sensi dell'art. 1 par. 2 della direttiva 98/34/CEE, modificata dalla direttiva 98/48/CEE. Nell'ipotesi in cui il social network fornisca dei veri e propri servizi di comunicazione elettronica, allo stesso si applicheranno anche le disposizioni della direttiva relativa alla vita privata ed alle comunicazioni elettroniche (2002/58/CEE"*. Così GALDIERI P., *Il trattamento illecito del dato nei "social network",* in *Giurisprudenza di merito,* 2012, n. 12, pag. 2699, richiamando la risoluzione sulla tutela della privacy nei servizi di social network (adottata in occasione della trentesima conferenza internazionale dei Garanti della privacy e della protezione dei dati a Strasburgo il 17 ottobre 2008).

commerciale di queste piattaforme che, negli ultimi anni, hanno effettivamente moltiplicato le capacità di comunicazione e pubblicizzazione: in che modo si potrebbe parlare del pericolo concreto di codesta fattispecie se non fosse possibile accertarlo "concretamente", anche se in seno ad una sterminata pluralità di utenti? Bisognerebbe ritornare ad una concezione di pericolo astratto, o dire, per assurdo, che il pericolo concreto sarebbe giustificato *in re ipsa*?

Ulteriori profili problematici si instaurano, qualora si analizzasse il medesimo fenomeno dal punto di vista opposto.

Ci si sofferma nuovamente sulla figura del soggetto attivo, chiedendosi se commette il reato chi utilizzi il dato di un altro soggetto senza il suo consenso[68]; si richiama inoltre l'articolo 5, comma 3°, del presente Codice, per cui il trattamento di dati effettuato da persone fisiche per fini esclusivamente personali soggiace all'applicazione del Codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Il Codice tuttavia, sebbene specifichi, come visto *supra,* il significato di comunicazione, non definisce il concetto normativo di comunicazione sistematica. Per giungere ad una soluzione soddisfacente, si deve richiamare il concetto di "esenzione domestica" desumibile della direttiva 95/46/CE[69]. Sulla base di quanto detto, si potrebbe dire che il trattamento di dati personali da parte dell'utente potrà considerarsi tale, potendo quindi rientrare nell'articolo 167, allorquando il soggetto in questione sarà in grado, trattando dati altrui tramite il proprio profilo online, di poterli diffondere ad *incertae personae*. È evidente però, come una posizione di questo tipo sia assolutamente carente sotto il profilo della determinatezza. Quale sarà allora il criterio da seguire per escludere una

… e nei confronti di un singolo utente

[68] Un esempio banale: Tizio, leggendo sul profilo online dell'amico Caio che questi ha sfortunatamente contratto una grave malattia, lo spiffera allegramente sulla proprio pagina del profilo senza il consenso dell'altro, condividendo la notizia con oltre 500 persone.

[69] Che all'art. 3 comma 2° prevede che le disposizioni della direttiva non si applichino al trattamento dei dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

comunicazione sistematica[70]? Nessuna pronuncia ha affrontato di petto questo tema, bensì solo collateralmente, ritenendo semplicemente che qualunque soggetto che operi nei social network sia tenuto ad osservare le disposizioni del Codice, fra cui l'obbligo di consenso al trattamento, la cui violazione potrebbe comportare l'applicazione dell'articolo 167, solo quando i dati raccolti e trattati siano destinati alla comunicazione sistematica ed alla diffusione[71]. Il vero problema è che, nonostante la stessa sottoscrizione ad un *social network*, raccolga dentro di sé l'insita volontà del soggetto a condividere una porzione della propria vita privata con altri, ciò tuttavia non gli garantisce che egli non possa ritrovarsi esposto[72], tanto da arrecargli nocumento, con inevitabili ripercussioni sulla sua sfera privata.

In casi di questo tipo, lo stesso concetto di esenzione domestica dovrebbe crollare: può essere sufficiente una valutazione numerica (le persone con cui si condivide un dato) in considerazione di aspetti della vita privata così personali da richiamare lo strato più profondo del diritto alla riservatezza? Tra l'altro non si dimentichi che il reato in questione è azionabile solo d'ufficio, mentre in casi di questo tipo sarebbe maggiormente convincente l'azionabilità tramite querela di parte; forse, come proposto da alcuni[73], la soluzione possibile potrebbe dunque essere quella di una revisione quantomeno parziale della disciplina, tramite l'introduzione di una selezionata cerchia di ipotesi delittuose caratterizzate dall'azionabilità tramite querela, nelle quali conseguentemente la violazione del diritto alla protezione dei dati personali non sia così grave da intaccare il nucleo essenziale di tale diritto.

---

[70] Ci si baserà sul numero degli utenti, lasciando pertanto pericolosi margini di discrezionalità al giudice, o, viceversa, si escluderà la sussistenza del delitto ogniqualvolta il profilo considerato sarà chiuso, ovvero con accesso limitato, ai soli "*followers*"?

[71] Cass. Pen., sez. III, 24 marzo 2011, n. 18909, come riporta GALDIERI P., *Il trattamento illecito del dato nei "social network",* in *Giurisprudenza di merito,* 2012, n. 12, pag. 2710.

[72] Di esempi ve ne sono un'infinità: chi inserisce sul proprio profilo le foto ritraenti l'immagine dei figli di una coppia amica, che mai inserirebbe le foto stesse sul proprio profilo; chi inserisce nel proprio profilo foto di amici, magari scattate nel corso di una festa in cui gli stessi appaiono in atteggiamenti non consoni all'età o alla professione che svolgono nel quotidiano.

[73] PICOTTI L., *I diritti fondamentali nell'uso ed abuso dei social network: aspetti penali,* in *Giurisprudenza di merito,* 2012, n. 12, pag. 2532.

1.2 Falsità nelle dichiarazioni e notificazioni al Garante (art. 168)

L'articolo 168 del presente Codice, rubricato "Falsità nelle dichiarazioni e notificazioni al Garante"[74], contiene il secondo delitto del D.lgs 196/2003 come originariamente previsto dall'art. 37-bis della L. 675/96, introdotto dall'art. 16 del D.lgs 467/2001.

La normativa extrapenale

Come si è anticipato, la norma è chiaramente posta a tutela del Garante Privacy, dal momento che il bene giuridico della riservatezza assume connotati di sola facciata, rilevando in primo piano il bene giuridico strumentale della trasparenza delle operazioni concernenti il Garante, così da "*precludere l'utilizzazione di atti o documenti suscettibili di fuorviarne le relative determinazioni, sulla base di erronei presupposti*"[75].

In questa fattispecie sono presenti nuovamente richiami alla disciplina extrapenale del presente Codice. L'art. 37 è relativo ai dati contenuti nella notificazione del trattamento, nei casi in cui essa costituisca un obbligo per il titolare. L'art. 32-bis, commi 1° e 8° invece, che è stato introdotto col D.Lgs 69/2012, concernente modifiche al Codice Privacy in materia di comunicazione elettronica, prevede, rispettivamente, la comunicazione "*senza indelebili ritardi*" al Garante del fornitore di servizi di comunicazione elettronica accessibili al pubblico in caso di violazione di dati personali e, nel caso in cui il fornitore di un servizio di comunicazione elettronica accessibile al pubblico affidi l'erogazione del predetto servizio ad altri soggetti, la comunicazione degli stessi al fornitore "*senza indebito ritardo*" di tutti gli eventi e le informazioni necessarie a consentire a quest'ultimo di effettuare gli adempimenti di cui al presente articolo. Infine, senza specifici richiami normativi, rileva anche qualsiasi comunicazione, atto, documento o

[74] Chiunque, nelle comunicazioni di cui all'art. 32-bis, commi 1 e 8, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

[75] Così MANNA A., *Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali,* in *Il diritto dell'informazione e dell'informatica,* n. 4-5, 2003, pag. 758.

dichiarazione reso e esibito in un procedimento dinanzi al Garante o nel corso di accertamenti.

Le condotte e il rapporto col falso ideologico e materiale

Quanto alle condotte incriminate, si considerano tali la dichiarazione o l'attestazione di false notizie o circostanze, ovvero la produzione di atti o documenti falsi. Risulta evidente come, in questo modo, siano state ricomprese sia le ipotesi di falso ideologico, che consiste nel dichiarare o attestare falsamente notizie o circostanze, sia quella di falso materiale, consistente invece nella produzione di atti o documenti falsi; difatti entrambe queste ipotesi sono state assimilate ai fini dell'applicazione della pena. Non a caso anche qui è presente la medesima clausola di riserva del trattamento illecito di dati, per cui si configura, ad esempio, concorso apparente di norme fra il presente articolo e l'art. 483 c.p. (falsità ideologica commessa dal privato in atto pubblico), fintanto che l'articolo 168 non solo è più grave, ma si pone anche in relazione di specialità rispetto la disposizione del Codice Penale.

Ulteriori profili del fatto tipico

Il soggetto attivo è "chiunque", tuttavia, per alcuni[76], dovrebbe trattarsi di un reato proprio o, quanto meno, a "soggettività ristretta"[77], poiché ne potrebbe rispondere il solo titolare del trattamento, obbligato ad effettuare comunicazioni e notificazioni. D'altro canto, s'è detto[78] come in realtà anche *l'extraneus,* può rispondere del delitto, anche a titolo di concorso, o comunque semplicemente in qualità di persona diversa dal titolare, tenuto conto che il presente Codice, quando ha voluto sviluppare esplicitamente dei reati propri, lo ha fatto espressamente, come all'articolo 169 e 170 ("Chiunque, essendovi tenuto").

Il reato si perfeziona quando vengono rilasciate le false dichiarazioni o nel momento in cui sono prodotti gli atti o i documenti falsi; di conseguenza, inquadrando la riservatezza come bene giuridico finale verso il quale il bene strumentale della trasparenza delle operazioni del Garante si erge a scudo, si

[76] CIRILLO G. P., *Il codice sulla protezione dei dati personali,* Milano, 2004, pag. 578.
[77] Si veda, sul tema, DEMURO G. P., *Il bene giuridico proprio quale contenuto dei reati a soggettività ristretta*, in *Riv. it. dir. proc. pen.*, II, 1998, p. 846.
[78] LUBERTO M., *I reati informatici contro il diritto alla privacy. La tutela fornita dal D.lgs 196 del 2003 e dal codice penale,* in *Giurisprudenza di merito,* n. 3, 2008, pag. 905.

deve necessariamente parlare di reato di pericolo astratto (o presunto), poiché non è necessario alcun pericolo concreto o lesione verso l'interesse tutelato; quindi, per esempio, ben può sussistere il reato se alla falsa notificazione non segua comunque un effettivo trattamento dei dati. Detto ciò, appare francamente opinabile la posizione di chi[79] ritiene comunque accettabile il tentativo, in forza del fatto che le condotte possono considerarsi frazionabili in più atti. Solitamente, ricomprendere il tentativo in reati di pericolo astratto o presunto comporta una accentuata forzatura, designando quella che è spesso definita come "anticipazione dell'anticipazione della tutela penale", vale a dire una significativa lesione al principio di offensività, attraendo indietro una volta in più la tutela offerta, cosa che già avviene configurando un reato di pericolo astratto o presunto.

Per ciò che riguarda, infine, l'elemento soggettivo, la norma richiede il solo dolo generico, vale a dire la consapevolezza nel soggetto agente della falsità delle notizie e dei documenti o delle attestazioni utilizzate, oltre che l'idoneità concreta a dare apparenza ingannevole a fatti e circostanze il cui accertamento o esistenza diventa rilevante all'interno di un procedimento di fronte al Garante.

[79] VILLANI C., *Le sanzioni penali,* in CUFFARO-D'ORAZIO-RICCIUTO, *Il codice del trattamento dei dati personali,* Giappichelli, 2006, Torino, pag. 749.

1.3 Misure di sicurezza (art. 169)

Il reato contenuto nel presente articolo è la prima contravvenzione del Codice Privacy, rubricata misure di sicurezza[80]. Esso mira a prevenire il verificarsi di pregiudizi nella sfera privata dei singoli, imponendo ai soggetti responsabili una serie di obblighi di protezione per la sicurezza delle informazioni. Nuovamente, sebbene il bene finale di tutela è la riservatezza dei singoli, permane in prima linea il bene strumentale della sicurezza del trattamento.

Si ritiene[81] comunque che la sicurezza del trattamento[82], come mezzo preventivo di tutela, svolga in ogni caso un ruolo fondamentale e ben maggiore rispetto a quei mezzi applicabili solo in seguito all'evento dannoso, per l'impossibilità di ripristinare lo stato antecedente alla lesione.

Il reato si perfeziona quindi senza alcun evento di danno, quando il soggetto che vi è tenuto omette di adottare le misure minime di sicurezza, trattandosi di conseguenza di un reato omissivo proprio, per cui il reato si considera di semplice condotta omissiva, punita a prescindere dal verificarsi di un evento naturalistico.

La normativa extrapenale

Circa il contenuto minimo delle "misure di sicurezza", è richiamato l'articolo 33 che, a sua volta, richiama artt. ulteriori quali il 31,34,35 ed il 58, comma 3°. Tramite combinato disposto, si desume che tali misure di sicurezza vengono

[80] 1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni.
2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

[81] VILLANI C., *Le sanzioni penali,* in CUFFARO-D'ORAZIO-RICCIUTO, *Il codice del trattamento dei dati personali,* Giappichelli, 2006, Torino, pag. 750.

[82] Si veda, in aggiunta, la posizione del Legislatore nella Relazione di accompagnamento al presente codice che motiva la previsione in esame *"per assicurare anche in sintonia con orientamenti giurisprudenziali internazionali in materia di diritti dell'uomo, la necessaria trasparenza alle tipologie di trattamenti effettuati epr tali finalità. In relazione ai tipi di operazioni e di dati oggetto del' trattamento e alle esigenze di aggiornamento e conservazione dei dati medesimi".*

individuate come segue: limitatamente ad alcuni soggetti[83], l'art.58, comma 3° prevede che le misure siano redatte dal Governo con apposito decreto del Presidente della Repubblica, con i conseguenti problemi precedentemente accennati in tema di norme penali in bianco[84], soprattutto per quanto riguarda il precetto ricavabile tramite atti normativi derivanti non dal potere legislativo, bensì dal potere esecutivo; per tutti gli altri titolari del trattamento, le misure di sicurezza sono individuate nell'Allegato B[85] del presente Codice, che fornendo specificazioni prettamente tecniche, rispetta i principi in tema di norma penale in bianco.

Il soggetto attivo

Per quanto attiene alla figura dei "soggetti responsabili", appare evidente che il reato in questione sia un reato proprio ("chiunque, essendovi tenuto"): il titolare del trattamento è il destinatario diretto di tutte quelle prescrizioni che sono richiamate nella contravvenzione in esame, dalle quali nasce una posizione di garanzia in senso formale. In aggiunta a ciò, rileva che in capo al titolare debba anche sussistere una responsabilità *in eligendo* ed *in vigilando*[86] tutte le volte in cui, per l'ampiezza dei suoi compiti, debba delegare a terzi lo svolgimento di alcune di queste attività, i quali potranno sempre essere chiamati a titolo di concorso.

Per quanto riguarda l'elemento soggettivo, trattandosi di contravvenzione, sarà richiesto indifferentemente il dolo o la colpa, inoltre, per lo stesso motivo, non

[83] L'art. 58, comma 1° prevede che essi siano gli organismi di cui agli articoli 3, 4 e 6 della legge 24 ottobre 1977, n. 801, ovvero sui dati coperti da segreto di Stato ai sensi dell'articolo 12 della medesima legge; essi sono: il Comitato esecutivo per i servizi di informazione e di sicurezza (CESIS), il Servizio per le informazioni e la sicurezza militare (SISMI), il Servizio per le informazioni e la sicurezza democratica (SISDE).

[84] Sebbene nel caso di specie il rinvio a norma secondaria sia apprezzabile, per la sua natura unicamente tecnica, meno apprezzabile è la provenienza di tale normativa dall'esecutivo, andando necessariamente contro il principio di legalità della legge penale, la questione tuttavia, non è pacifica: si veda, *a contrario,* Corte Cost.,sent. n. 113 del 1972; nonché sent. n. 282/1990.

[85] Tale allegato tratta esplicitamente il disciplinare tecnico in materia di misure di sicurezza, ad esempio: che gli incaricati abbiano un codice identificativo pèrsonale e una password, che i programmi antivirus siano aggiornati almeno semestralmente, che i dati vengano salvati almeno una volta a settimana, ecc.

[86] La responsabilità in *eligendo* prevede il dover scegliere con cura quelle persone dotate di esperienza necessaria, capacità d' affidabilità che diano una garanzia idonea rispetto le disposizioni vigenti in materia di trattamento, nei confronti delle quali venga eventualmente delegata parte dei propri compiti. La responsabilità in *vigilando* ricomprende un generale dovere di sorveglianza da parte del delegante verso le attività del delegato.

sarà configurabile il tentativo, dal momento che esso è espressamente previsto solo per i delitti.

L'insolita estinzione del reato

Infine, circa il comma 2°, è prevista una causa di estinzione del reato, che riprende parte della disciplina prevista nella legislazione sugli infortuni sul lavoro; allo stesso tempo essa si distingue dalla oblazione, poiché la sanzione di riferimento non è un ammenda, bensì una sanzione amministrativa. In seguito al compimento del reato, accertata la violazione da parte del Garante e imposte all'autore del reato determinate prescrizioni sulle suddette misure, tale soggetto può, entro sessanta giorni[87] dalla scadenza del termine fissato dal Garante stesso, estinguere il reato se regolarizzi la propria posizione adempiendo a tutte le prescrizioni imposte dall'autorità e versando inoltre una somma pari a un quarto del massimo sella sanzione amministrativa[88]. Di fronte ad un'estinzione del reato così singolare, con conseguente depenalizzazione del fatto, parte della dottrina[89] ha giustamente rilevato che sarebbe stato molto più semplice convertire anche questo illecito da penale ad amministrativo, soprattutto se rapportato ai principi di frammentarietà, sussidiarietà ed *extrema ratio* del diritto penale.

[87] Che possono sensibilmente aumentare tramite proroga dell'autorità qualora si rinvengano casi di particolare complessità o per l'oggettiva difficoltà dell'adempimento, ma che mai può superare i sei mesi.

[88] All'art. 162 comma 2-bis, in tema di sanzioni amministrative è previsto che in caso di trattamento di dati personali effettuato in violazione delle misure indicate nell'articolo 33 è altresì applicata in sede amministrativa la sanzione del pagamento di una somma da diecimila euro a centoventimila euro. Di conseguenza, tramite un contorto giro legislativo, si è imposta una sanzione amministrativa in aggiunta all'arresto della contravvenzione in esame che però, allo stesso tempo, diventa elemento di calcolo in tema di estinzione del reato, dando vita ad una singolare commistione di elementi penali e amministrativi. Il problema in questione è sorto quando, nel 2009, con L. n. 14, fu eliminata l'ammenda nel presente articolo, lasciando semplicemente l'arresto.

[89] MANNA A., *Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali,* in *Il diritto dell'informazione e dell'informatica,* n. 4-5, 2003, pag. 765.

1.4 Inosservanza di provvedimenti del Garante (art. 170)

L'articolo 170[90] del presente Codice è il terzo ed ultimo delitto nel titolo relativo alle sanzioni, posto nuovamente a tutela della figura del Garante, intendendosi come bene giuridico strumentale di tutela quello della funzione di controllo del Garante per la protezione dei dati personali.

La disposizione riprende per intero la medesima fattispecie dell'antecedente L. 675/96, con l'aggiunta del riferimento normativo all'art. 90, relativo al trattamento di dati genetici in ragione della particolare delicatezza della materia[91]. Tra l'altro, attraverso la già esaminata tecnica del rinvio, il legislatore ha deciso di circoscrivere l'area di provvedimenti del Garante rilevanti ai fini di questa fattispecie, ai soli considerati di una certa gravità.

La normativa extrapenale

Il primo riferimento normativo concerne il mancato rispetto delle indicazioni che seguono il rilascio dell'autorizzazione al trattamento dei dati sensibili, considerati tali da richiedere una maggiore protezione rispetto a quelli comuni in ragione della maggiore capacità offensiva che potrebbe scaturire da un eventuale condotta dannosa verso questi. Il secondo tratta invece l'inosservanza delle prescrizioni contenute nella decisione finale del ricorso[92].

Il terzo infine disciplina l'inosservanza delle misure cautelari infraprocedimentali[93].

È evidente come il legislatore, in questo modo, abbia rafforzato, con finalità preventiva, il valore delle decisioni del Garante, sfruttando il presidio della

[90] Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni.

[91] È questa la motivazione data nella relazione di accompagnamento del Codice Privacy.

[92] L'art. 150, rubricato provvedimenti a seguito del ricorso, disciplina il provvedimento del Garante che scaturisce, nelle condizioni del presente articolo, a seguito di ricorsi da parte degli interessati che, ai sensi del presente Codice, ritengano violati i loro diritti.

[93] L'art. 143, comma 1, lettera c), prevede quanto segue: Il Garante dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera b), oppure quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati.

sanzione penale. Tuttavia, secondo alcuni[94], data la mancata unificazione legislativa fra i variegati tipi di provvedimenti richiamati, sarebbe stato anche possibile riconsiderarli all'interno del trattamento illecito di dati.

Conseguenza di ciò è che, nuovamente, si ripropone il problema delle norme penali in bianco, per cui è necessario chiedersi se il richiamo ai provvedimenti del Garante non sia tale da sperequare il rapporto fra tale fattispecie e i principi di tassatività e determinatezza; tuttavia parte della dottrina ha ritenuto che, in questo caso, un'eventuale censura di illegittimità costituzionale sarebbe eccessiva[95].

Ulteriori profili del fatto tipico

Il reato si perfeziona nel momento in cui scade il termine fissato per l'osservanza del provvedimento o, in mancanza di termine, nel momento in cui allo stesso provvedimento segua la condotta vietata, o, ancora, quando l'attività viene posta in essere in mancanza del provvedimento richiesto.

Come per l'articolo precedentemente affrontato, il soggetto attivo del reato è "chiunque, essendovi tenuto", ragion per cui deve trattarsi di un reato proprio, riassorbendo tutte le considerazioni delineate nel corso della fattispecie sulle misure di sicurezza.

Il reato risulta essere omissivo proprio, ragion per cui è difficilmente configurabile il tentativo.

Per quanto concerne l'elemento soggettivo, trattandosi ora di delitto, e non essendo altrimenti specificata una responsabilità colposa, esso risulta essere necessariamente doloso, richiedendosi la rappresentazione e volizione da parte del soggetto attivo di non voler osservare il provvedimento del Garante.

---

[94] Ritiene così DEL CORSO S., *La protezione dei dati personali,* a cura di BIANCA C. M., BUSNELLI F. D., CEDAM, 2007, Padova, pag. 2073.

[95] Nel dettaglio, è stato ritenuto che, innanzitutto, il contenuto di questa norma sarebbe individuato solamente a posteriori in base al provvedimento del Garante; inoltre tale articolo sarebbe del tutto assimilabile all'art. 388 del c.p. che presidia l'autorità delle decisioni giudiziarie in settori sensibili, proprio come l' art. 170 tutela le decisioni del Garante: LUCENTE C., *La nuova normativa penale a tutela dei dati personali,* in CARDARELLI-SICA-ZENO ZENOCOVICH, *Il codice dei dati personali. Temi e problemi,* Milano, 2004, pag. 653 e ss.

1.5 Altre fattispecie (art. 171)

A conclusione del capitolo concernente l'analisi dei reati privacy propri, permane lo studio dell'articolo 171[96], ultima fattispecie prevista nel presente titolo. La condotta punita, di difficile comprensione tramite la semplice lettura di tale articolo, nonché la singolare rubrica utilizzata, è il trattamento effettuato in violazione delle disposizioni concernenti, rispettivamente, la raccolta di dati e pertinenza ed il divieto di controllo a distanza e telelavoro. Trattasi di una contravvenzione, in quanto la violazione, prevista tramite richiamo alla disciplina dei lavoratori, è punita con l'ammenda o l'arresto.

Il primo caso è previsto tramite il richiamo all'articolo 113 del presente Codice che, tramite una torsione inspiegabile, rinvia ulteriormente all'art. 8 della legge n. 300/1970, cd. Statuto dei lavoratori. In esso è previsto un espresso divieto al datore di lavoro di effettuare, sia ai fini dell'assunzione che nel corso del rapporto di lavoro, indagini su opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione della sua attitudine professionale.

Il secondo caso, presente nell'articolo 114 che propone il medesimo richiamo all'art. 4 dello Statuto dei lavoratori, prevede che sia vietato[97] al datore di lavoro di utilizzare impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza dei lavoratori.

---

[96] La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300.

[97] C'è da dire, che è considerato tuttavia doveroso il controllo del traffico telematico aziendale da parte dell'imprenditore. Alcuni casi sono espressamente previsti dalla legge, come quello della necessità per l'azienda di ovviare al rischio di una propria responsabilità in conseguenza di fatti illeciti dei propri dipendenti. Il problema, di conseguenza, si sposta sui limiti del controllo in questione. A ben vedere, infatti l'art. 4 dello Statuto dei Lavoratori distingue ipotesi di divieto assoluto e relativo. Il divieto assoluto, al comma 1°, riguarda gli impianti e le altre apparecchiature (intesa come categoria aperta comprendente anche strumenti informatici e telematici) atte a realizzare u controllo a distanza intenzionale de l lavoratore. Il divieto relativo, al comma successivo, concerne il controllo preterintenzionale, ciò è effettuato con l'installazione di impianti ed apparecchiature richieste da esigenze organizzative o concernenti al sicurezza del lavoro nei quali la possibilità del controllo a distanza del lavoratore è solo eventuale. A riguardo si veda, in dettaglio ROSSI V., *Divieto di controllo a distanza e telelavoro,* in *Codice in materia di protezione dei dati personali,* Vicenza, 2004, pag. 523.

Come è ovvio, trattasi di reato proprio, in quanto può essere commesso solo da chi rivesta la qualifica di datore di lavoro. Il bene giuridico tutelato, invece, è decisamente quello della riservatezza nonché delle libertà sindacali del lavoratore a non essere discriminato nel luogo di lavoro. Tuttavia non sembra corretto definirlo quale reato di natura plurioffensiva, in quanto è possibile ritenere tali libertà come rientranti nel concetto di privatezza del singolo, tutelato dal bene giuridico della riservatezza.

Trattandosi di reato contravvenzionale, esso potrà essere commesso indipendentemente con dolo o con colpa e, inoltre, non sarà configurabile il tentativo.

Per quanto concerne le sanzioni, vi è un ulteriore rinvio all'articolo 38 dello Statuto dei lavoratori, che si sviluppa in tre commi[98]. Rileva, come curiosità, il fatto che, nonostante le sanzioni penali del presente Codice siano caratterizzate da pubblicità della sentenza solo se sono delitti, il caso del presente articolo prevede comunque tale pubblicità, ai sensi del rinvio allo Statuto del Lavoratori.

È evidente come l'articolo in questione contenga una caratteristica davvero peculiare in quanto, non solo il precetto, ma anche la sanzione, sono individuati tramite un richiamo ad una normativa esterna al presente Codice.

[98] È prevista l'ammenda da euro 154,95 a euro 1.549,50 o l'arresto da 15 giorni ad un anno. Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente. Quando per le condizioni economiche del reo, l'ammenda stabilita nel primo comma può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo. Nel secondo caso, l'autorità giudiziaria ordina la pubblicazione della sentenza penale di condanna nei modi stabiliti dall'articolo 36 del codice penale.

CAPITOLO IV – I REATI PRIVACY IMPROPRI: IL CODICE PENALE

1. I reati privacy impropri del Codice Penale: reati non informatici e reati informatici - 1.1 Reati non informatici: violazione di domicilio e violazione di domicilio commessa da un pubblico ufficiale (artt. 614, 615) - 1.2 Interferenze illecite nella vita privata (art. 615 bis) - 2.1 Reati informatici: accesso abusivo ad un sistema informatico o telematico: premessa (art. 615 ter) - 2.1.1 Il dibattito sul bene giuridico tutelato - 2.1.2 La struttura del reato - 2.1.3 Il significato di «sistema informatico e telematico protetto da misure di sicurezza» - 2.1.4 Le condotte rilevanti - 2.1.5 Il requisito dell'abusività - 2.1.6 Altri aspetti rilevanti della fattispecie - 2.2 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater) - 2.3 Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies) - 2.4 Violazione della corrispondenza e delle comunicazioni telefoniche, informatiche e telematiche (art. 616, 617 - 617 sexies) - 2.5 Danneggiamento di informazioni, dati e programmi e sistemi informatici(635 bis, 635 ter, 635 quater, 635 quinquies) - 2.6 Frode informatica e «phishing»: premessa e ratio della norma (art. 640 ter) - 2.6.1 La struttura del reato e le modalità di condotta - 2.6.2 L'ingiusto profitto e l'altrui danno; l'elemento soggettivo, le circostanze aggravanti e i rapporti con altri reati - 2.6.3 Il «phishing»: il significato e la recente sentenza di Cassazione n. 9891 del 2011

1. I reati privacy impropri del Codice Penale: reati non informatici e reati informatici

Nel corso del presente capitolo saranno analizzati i cd. reati privacy impropri o in senso lato[1], intendendosi per tali quei reati che, in tutto o in parte, tutelano il bene giuridico della privacy sebbene non siano inseriti all'interno del rispettivo Codice della Privacy, bensì all'interno del Codice Penale.

Introduzione

Trattasi di fattispecie che indicativamente non tutelano in via diretta la riservatezza, poiché sviluppate come reati plurioffensivi. Tra i beni giuridici tutelati si segnalano, ad esempio, il domicilio informatico, la segretezza informatica, la tranquillità delle persone, il patrimonio, ecc.

A sua volta i reati privacy impropri possono scindersi in reati privacy non informatici e informatici; nel Codice Penale, infatti, gli artt. 614, 615 e 615-bis sono posti a tutela di un concetto di riservatezza dalle origini più antiche che

[1] Dizione utilizzata, in contrapposizione ai reati privacy propri, da LUBERTO M., *I reati informatici contro il diritto alla privacy. La tutela fornita dal D.lg. n.196 del 2003 e dal Codice Penale,* in *Giurisprudenza di merito,* 2008, 3, pag. 909.

moderne, poiché ci si appresta a fornire tutela al domicilio degli individui, sottolineandone l'aspetto prettamente materialistico. Molti altri reati sono, invece, posti a tutela di beni giuridici, fra cui la riservatezza, intrinsecamente collegati con ambiti prevalentemente informatici; si pensi all'art. 615-ter[2] che, tutelando il domicilio informatico, è sostanzialmente slegato da aspetti puramente materiali. Molto, su questo aspetto, come si avrà presto modo di analizzare, è stato introdotto con la legge n. 547 del 1993 e con la legge n. 48 del 2008, di ratifica della Convenzione di Budapest[3] del 2001.

[2] Il quale, tra le alte cose, fu il primo reato informatico introdotto nel Codice Penale, dalla legge 547/93 che espressamente, senza il bisogno di operazioni giurisprudenziali su altri articoli, tutelava il cd. domicilio informatico.

[3] Trattasi della storica Convenzione del Consiglio d'Europa sulla criminalità informatica, avvenuta a Budapest il 23 novembre 2001.

1.1 Reati non informatici: violazione di domicilio e violazione di domicilio commessa da un pubblico ufficiale (artt. 614, 615)

La violazione di domicilio[4] è disciplinata dall'art. 614 del Codice Penale, Sezione IV (dei delitti contro l'inviolabilità del domicilio), capo III (dei delitti contro la libertà individuale), titolo XII (dei delitti contro la persona) del libro Secondo (dei delitti in particolare).

Art. 614 c.p.: Il bene giuridico tutelato

Il bene giuridico tutelato, in primissimo piano, è quello della libertà domiciliare dell'individuo, che riceve, come si è visto, immediata tutela costituzionale, quale diritto fondamentale, all'art. 14[5]. Esso viene ricompreso nel più ampio concetto della libertà individuale[6], dal quale discende, fra gli altri, il famoso principio dello *ius excludendi alios,* tanto caro ai lontani – ma tutt'ora validi – orientamenti analizzati *supra* in tema di riservatezza. Si ritiene[7], infatti, che in questo concetto sia pienamente in grado di rientrare un diritto alla riservatezza domiciliare, che si configura come strumentale alla libera manifestazione della personalità, che quindi non consente ad altri di prendere conoscenza di ciò che avviene nella sfera privata domiciliare se non nei casi previsti dalla legge.

Per quanto a noi interessa, dunque, non sembra corretto, in tal caso, arrivare a parlare di plurioffensività della fattispecie, in quanto l'interesse della

---

[4] 1. Chiunque s'introduce nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle appartenenze di essi, contro la volontà espressa o tacita di chi ha il diritto di escluderlo, ovvero vi s'introduce clandestinamente o con inganno, è punito con la reclusione da sei mesi a tre anni.
2. Alla stessa pena soggiace chi si trattiene nei detti luoghi contro l'espressa volontà di chi ha il diritto di escluderlo, ovvero vi si trattiene clandestinamente o con inganno.
3. Il delitto è punibile a querela della persona offesa.
4. La pena è da uno a cinque anni, e si procede d'ufficio, se il fatto è commesso con violenza sulle cose, o alle persone, ovvero se il colpevole è palesemente armato.

[5] Ma non solo, si ricorda infatti che esso ha espressa tutela anche nell'art. 12 della Dichiarazione universale dei diritti dell'uomo e all'art. 8 della CEDU.

[6] Sul tema del domicilio si veda, nello specifico, SINISCALCO E., *Domicilio* (violazione di), in ED, XIII, Milano, 1964, 871 e MUSACCHIO V., *Violazione di domicilio*, in *Digesto pen*., XV, Torino, 1999, pag 228.

[7] Su tutti, così ritiene ANTOLISEI F., *Manuale di Diritto Penale – Parte Speciale I,* Milano, Giuffrè Editore, 2003, pag. 231.

riservatezza, per il suo aspetto materiale e domiciliare, viene ricompreso nel più ampio diritto alla libertà individuale nel suo ambito spaziale.

La fattispecie in questione vanta, da sempre[8], una tutela penale consistente, ma è solo col Codice Rocco prima, e con la Costituzione poi, che viene arricchita ulteriormente così da comprendere non solo la pace domestica, ma anche tutte le altre manifestazioni di libertà che sono estrinsecazione della vita privata della persona tra le quali, come si è detto, la riservatezza domiciliare. Circa il concetto di domicilio, secondo quando ritiene la prevalente dottrina, la Costituzione non fornisce *"indicazioni di contenuto suscettibili di precisare una nozione tipica ed autonoma di domicilio, limitandosi ad apprestare un particolare meccanismo di garanzia attraverso il rinvio a definizioni già contenute in fattispecie normative preesistenti"* [9]; per questa ragione, la nozione penale di domicilio, rileverà in modo autonomo e più ampio rispetto a quella di altri settori dell'ordinamento, come ha previsto, in modo costante negli anni, la giurisprudenza di legittimità[10]. Il delitto in esame circoscrive l'area del domicilio ai concetti di abitazione, altro luogo di privata dimora e appartenenze di essi.

La nozione di domicilio

Per il primo, si è soliti intendere ogni luogo dove la persona dimori legittimamente e in modo attuale, da solo o con altri[11], in modo da avere conseguentemente il diritto di escludere chiunque non sia autorizzato ad entrarci. Il secondo è necessariamente più ampio, in quanto ricomprende, per esclusione, ogni luogo anche diverso dall'abitazione, ove si svolga qualsiasi attività della vita privata che si compia al riparo dalle ingerenze altrui[12]. Il

[8] Un punto di svolta si è sicuramente registrato con la Rivoluzione Francese a seguito della quale ha acquistato ampia espansione il diritto della libertà individuale. Per quanto concerne l'antico Codice Zanardelli, si considerava reato soltanto qualora conseguisse un attentato alla pace domestica dell'individuo, mentre come detto, col Codice attuale, la dizione si è conseguentemente ampliata.

[9] BORRELLI G., *Riprese filmate nel bagno di un pubblico esercizio garanzie costituzionali*, in *Cassazione Penale*, 2001, pag. 2453.

[10] Cass. Pen., Sez. III, n. 1451 del 1968 ; Cass. Pen., Sez. III, n. 6316 del 1983 ; Cass. Pen. Sez. V, n. 35166 del 2005; Cass. Pen., Sez. III, n. 46191 del 2008.

[11] La casa, il palazzo, ma anche una caverna, una tenda, una baracca.

[12] Sono tali lo studio professionale, una camera d'albergo, il bar, un negozio, la cabina di una nave. Si cita una recente sentenza di Cassazione n. 41646 del 2013 per la quale *"esso comprenda qualunque luogo, anche se diverso dalla casa di abitazione, in cui la persona si soffermi per compiere, pur se in*

terzo, invece, ricomprende tutti quei luoghi che integrano in senso sia logistico che di servizio, per necessità o anche solo per eventualità, la funzione che l'abitazione o il luogo di privata dimora svolge per il soggetto che ne dispone, così da consentirgli di escludere gli altri da intromissioni che violino la vita domestica o privata[13]. Infine, ognuno di questi concetti deve anche soddisfare alcuni requisiti quali l'attualità dell'uso[14] e la legittimità dell'uso[15].

Le condotte punite

Venendo alle condotte dell'articolo 614, esse consistono alternativamente nell'introdursi o nel trattenersi all'interno dei luoghi analizzati pocanzi contro la volontà di chi abbia il potere di escluderli (detto anche *invito domino*). L'introduzione può avvenire semplicemente tramite la porta di ingresso, o anche in via anomala, come dal balcone o dalle finestre fintanto ciò sia in grado di ledere il diritto alla esclusività e riservatezza del titolare dello *ius excludendi*. Sul punto si è detto[16] che *"l'introduzione anche solo parziale di una parte del corpo nell'altrui domicilio, sia diversamente qualificabile come tentativo o come delitto consumato in ragione, non già di una valutazione di tipo volumetrico della intrusione, bensì alla luce di una valutazione che tenga conto della effettiva potenzialità lesiva della condotta realizzata nei confronti del bene 'riservatezza domiciliare' tutelato dalla norma"*. Da ciò si evince giustamente come, ad esempio, chi, per origliare, si appresti ad introdurre solo la testa nella finestra della casa del vicino, per sentirne discorsi piccanti, potrebbe consumare il delitto, mentre, chi tenta di raggiungere il balcone adiacente, venendo colto sul fatto, sarà punito eventualmente per il tentativo. Con l'atto di trattenersi si intende, invece, la permanenza *invito domino*

---

modo contingente e provvisorio, atti della sua vita privata riconducibili al lavoro, al commercio, allo studio, allo svago".

[13] In questo concetto talvolta sono state fatte rientrare anche appartenenze che siano comuni a più luoghi di abitazione o di privata dimora, come pianerottoli, giardini condominiali e atri.

[14] Da intendersi come fruizione dell'abitazione per lo svolgimento della vita domestica, non necessariamente in modo continuativo. Come è ovvio, non è stato fatto rientrare in questo concetto l'appartamento disabitato.

[15] Vale a dire un titolo legittimo, come la proprietà o l'usufrutto o anche una situazione di fatto riconosciuta dall'ordinamento come la convivenza o la detenzione.

[16] MANTOVANI F., *Diritto Penale – Parte Speciale, delitti contro la persona,* Padova, 2012, pag. 434; *contra* ANTOLISEI per il quale è richiesta la totalità della persona all'interno del domicilio per consumare il reato.

dell'individuo nel domicilio altrui, presupponendo necessariamente un ingresso precedente avvenuto lecitamente a cui consegue un invito ad allontanarsi. Invece, per quanto concerne l'introduzione, essa può avvenire avverso uno *ius prohibendi* espresso (gesti, parole, scritte) o tacito[17] (cancelli, porta chiusa a chiave) del soggetto passivo. Tali condotte permangono anche se conseguite clandestinamente o con l'inganno[18], vale a dire eludendo la vigilanza del titolare o mediante lo sfruttamento di veri e propri mezzi fraudolenti (come delle false generalità).

Ulteriori profili del fatto tipico

Venendo al perfezionamento della fattispecie, la quale, è un reato di danno, esso si avrà, come reato istantaneo, nel momento in cui avviene l'ingresso o, nel caso del trattenimento abusivo, quando l'agente comincia ad intrattenersi nel domicilio, come reato permanente; conseguentemente il tentativo è pienamente configurabile.

Per quanto concerne l'elemento soggettivo, è richiesto il dolo generico, intendendosi la coscienza e volontà di introdursi o trattenersi in un luogo che costituisce altrui domicilio contro la volontà di chi ne sia titolare, non rilevando dunque il fine.

Soffermandoci sul significato della querela, in questo reato essa dev'essere proposta dal soggetto passivo del reato, vale a dire il titolare dello *ius*

[17] Rimane invece controverso, sia in dottrina che in giurisprudenza, il valore del dissenso presunto. Si pensi al caso dell' introduzione in assenza del titolare o a sua insaputa per cui il dissenso non sia stato esplicitato, per la situazione concreta, per ignoranza o per effetto del comportamento ingannevole altrui, ma che poteva ragionevolmente presumersi: LA CUTE G., *Il dissenso presunto nel reato di violazione di domicilio*, in *Riv. Pen*., 1989, 1041 non condivide la teoria del dissenso presunto, ritenendo che, in linea col principio di tassatività, la locuzione adottata dall'art. 614, richiedendo una contraria volontà "espressa o tacita" sembrerebbe volere sempre una manifestazione del dissenso anche se per *facta concludentia. Contra* invece MAGGIORE G., *Diritto penale – Parte Speciale,* Vol. II., pag. 891 il quale ritiene che il consenso e il dissenso è presunto ogni qual volta che *"le circostanze di fatto con speciale riguardo al comportamento del titolare e alla sua personalità, rendano assurda l'ipotesi del consenso di questo, in vista del fine illecito del colpevole"*.

[18] A questo fine, specificatamente con finalità illecite, di interessante rilievo è una recente sentenza di Cassazione n. 19546 del 2013 in cui si è distinta l'ipotesi dell'agente che frequenti il domicilio per ragioni di amicizia o parentela, da quella in cui l'autorizzazione non c'è ed in cui l'agente renda l'esistenza di quel fine non percepibile da parte del titolare dello *ius exludendi*. Nel primo caso ricorrerebbe l'ipotesi di introduzione nel domicilio altrui contro la volontà tacita del titolare ritenendosi implicita, in presenza di quel fine, la contraria volontà del titolare e a nulla rilevando l'assenza di clandestinità; nel secondo caso, invece, si tratterebbe di introduzione con inganno poichè il principio della non presumibilità del dissenso del titolare vale solo a scriminare la condotta di chi operi in situazioni tali da far ragionevolmente ritenere che dissenso non vi sia.

excludendi. Inoltre, si è detto che a fronte di una pluralità di titolari, se si tratterà di una comunità organizzata, il potere spetterà a chi è investito del potere di direzione mentre, in ambito ad esempio familiare, tale *ius* spetta indistintamente a tutti coloro i quali abitano nel domicilio oggetto di intromissione[19].

Un'ultima considerazione è richiesta circa il comma 4° che prevede la procedibilità d'ufficio e l'aumento di pena se il fatto è commesso con violenza sulle cose o su persone o se il colpevole è palesemente armato. Esse conseguentemente danno vita ad un reato complesso[20] in grado di assorbire i reati di danneggiamento e violenza privata con conseguente esclusione del cumulo delle pene. Qualora tali circostanze avvenissero simultaneamente si ritiene in modo unanime che sia da escludere il fenomeno del concorso poiché l'articolo in questione individua una norma a più fattispecie[21].

Dunque, come si è avuto modo di vedere, la fattispecie in questione non fa altro che incarnare, all'interno del bene giuridico della libertà individuale, l'anima nativa del diritto alla riservatezza, figlio del diritto del proprietario di escludere chiunque al di fuori della sua abitazione, proprio come nel caso precedentemente analizzato di Warren e Brandeis.

L'art. 615 c.p.

L'articolo sinora studiato che, trattava un reato comune, si contrappone all'articolo successivo, 615 c.p.[22], rubricato violazione di domicilio commessa da un pubblico ufficiale, che si configura invece come reato proprio.

[19] Così SINISCALCO E., *Domicilio* (violazione di), in ED, XIII, Milano, 1964, pag. 877.

[20] L'art. 84 del Codice Penale prevede che quando un fatto che di per sè stesso costituisce reato è considerato da una disposizione di legge come elemento costitutivo o circostanza aggravante di un altro reato, si applica solamente la disposizione in questione. Con questa figura giuridica si da vita ad una riunione di più reati in uno soltanto, con i rispettivi aumenti di pena. ANTOLISEI F., *Manuale di Diritto Penale – Parte speciale I,* Milano, Giuffrè Editore, 2003, pag. 537.

[21] E non, invece, una fattispecie a più norme, fenomeno che caratterizza, in un'unica disposizione legislativa, la presenza di più reati, benché in un unico articolo.

[22] 1. Il pubblico ufficiale, che, abusando dei poteri inerenti alle sue funzioni, s'introduce o si trattiene nei luoghi indicati nell'articolo precedente, è punito con la reclusione da uno a cinque anni.
2. Se l'abuso consiste nell'introdursi nei detti luoghi senza l'osservanza delle formalità prescritte dalla legge, la pena è della reclusione fino a un anno.

Come si evince dalla fattispecie, viene ripreso in gran parte il contenuto dell'articolo precedente, difatti, permane, come bene giuridico tutelato, la libertà domiciliare, alla quale, però, si aggiunge l'interesse al corretto esercizio dei poteri pubblici, costituendosi dunque come reato plurioffensivo caratterizzato da una maggiore gravità rispetto alla semplice violazione di domicilio.

Il soggetto attivo ed il dibattito sulla condotta del comma 2°

Circa il soggetto attivo che, come detto, dà vita ad un reato proprio, si è evidenziato[23] come non sembra corretto aver escluso la figura dell'incaricato di un pubblico servizio per questa fattispecie; l'incaricato potrà essere punito per il solo art. 614 con l'aggravante dell'art. 61 n. 9 c.p.[24], nonostante si ritiene che, fra le due figure, sia avvenuta una sostanziale parificazione con l'ampliamento della responsabilità penale agli incaricati di pubblico servizio.

Le condotte punite sono due, l'introduzione o l'intrattenimento del pubblico ufficiale tramite l'abuso[25] dei poteri interenti alle sue funzioni e l'introduzione senza il rispetto delle formalità previste dalla legge. Per quanto riguarda la prima, si ritiene che l'abuso debba essere strumentale alla violazione del domicilio, ed è infatti per questo motivo che manca il riferimento alla volontà contraria del titolare dello *ius excludendi*[26]. Circa la seconda, si ritiene che la condotta di introduzione nell'altrui domicilio si costituisca mediante una specifica e meno grave forma di abuso, consistente nella inosservanza delle formalità prescritte dalla legge per legittimare l'intrusione; dunque, in questo secondo caso, l'introduzione sembra essere di per sé lecita, ma subordinata a determinate forme di legge. Dal momento che l'inosservanza delle formalità non è un nuovo elemento che si aggiunge alla fattispecie ma, come ritiene

[23] Così ANTOLISEI F., *Manuale di Diritto Penale – Parte speciale I,* Milano, Giuffrè Editore, 2003, pag. 242.

[24] "L'aver commesso il fatto con abuso dei poteri, o con violazione dei doveri inerenti a una pubblica funzione o a un pubblico servizio, ovvero alla qualità di ministro di un culto".

[25] Che può appalesarsi nell' eccedere i limiti della propria competenza, usare il potere conferitogli per finalità diverse da quelle per cui questo gli è stato attribuito, superare i limiti fissati dalla legge per disciplinarne l'esercizio, violare gli obblighi impostigli per il corretto esercizio di tale potere.

[26] Può farsi l'esempio dell'ufficiale di polizia giudiziaria che avvalendosi della sua qualità, compie una perquisizione domiciliare fuori dai casi consentiti dal codice di procedura penale.

Antolisei, una forma particolare di abuso, la condotta del comma 2° è semplicemente una disposizione speciale rispetto a quella precedente[27].

Anche per questo reato, l'elemento soggettivo richiesto è il dolo generico, concretizzandosi nella coscienza e volontà di violare il domicilio altrui consapevole della qualifica rivestita e della condotta di abuso utilizzata strumentalmente.

Dunque, come si è avuto modo di vedere, entrambi i reati analizzati costituiscono certamente l'esempio più evidente di fattispecie poste a tutela della riservatezza, intesa come il potere di escludere dall'alveo della propria vita privata chiunque non abbia il diritto di accedervi, rientrando in questo modo nella definizione proposta *supra* di reati privacy in senso lato.

[27] *Contra* MANZINI V., *Trattato di diritto penale italiano,* vol. VIII, n.3153, UTET, 1986, pag. 862 per il quale invece il comma 2° costituisce una circostanza attenuante speciale rispetto alla condotta del comma 1°.

1.2 Interferenze illecite nella vita privata (art. 615 bis)

L'articolo 615 bis[28] tratta la fattispecie di interferenze illecite nella vita privata, riprendendo e successivamente allargando alcune caratteristiche rinvenibili nei due articoli precedenti. Di conseguenza è richiamato non solo l'art. 14[29] della Costituzione, ma anche il 15, relativo all'inviolabilità della segretezza, della corrispondenza e di ogni altra forma di comunicazione. Difatti anche il bene giuridico risulta allargato rispetto a quello relativo alla violazione del domicilio; si rimane all'interno del concetto della riservatezza domiciliare, ma si scavalca la mera normativa spaziale, ricomprendendo anche "*il divieto di captazione diretta o indiretta, come di divulgazione di ogni manifestazione di libertà della persona che in quei luoghi si compia*"[30]; tuttavia il bene giuridico della riservatezza tutelato in questa fattispecie è, nuovamente, preso in considerazione solo nella sua componente negativa (*libertà da*).

Il bene giuridico tutelato e rilevi di incostituzionalità

Preme immediatamente rilevare, sul piano costituzionale, prima di immergersi nelle questioni concernenti la fattispecie, alcuni rilievi di incostituzionalità relativi all'art. 226 comma 2° c.c.p. e l'art. 14 Cost. Tale disposizione consente infatti di effettuare intercettazioni di comunicazioni tra presenti, avvenute nei luoghi di privata dimora, se vi sia il fondato motivo di ritenere che in quei luoghi si stia svolgendo un'attività criminosa; in particolari

---

[28] 1. Chiunque mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni.
2. Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo.
3. I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato.

[29] Senza ribadire i già citati artt. 12 della Dichiarazione Universale dei diritti dell'uomo e 8 CEDU.

[30] Così BRICOLA F., *Prospettive e limiti della tutela penale della riservatezza,* in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Milano, Giuffrè, 1970, p. 1083 poi ripreso da MANTOVANI F., *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Milano, Giuffrè, 1970, p. 405.

pronunzie si è obbiettato che ciò realizzerebbe una violazione della riservatezza domiciliare potendo eventualmente integrare il reato qui in esame dal momento che sono assenti nella normativa specifici parametri per stabilire le modalità delle intercettazioni domiciliari. Tuttavia, per il momento tali pronunce si sono fermate al giudice di merito, senza raggiungere la Corte Costituzionale, difatti, come ha rilevato la Cassazione[31] la collocazione di microspie all'interno di un luogo di privata dimora costituisce una delle modalità di attuazione delle intercettazioni, essendo queste un mezzo di ricerca della prova funzionale al soddisfacimento dell'interesse pubblico all'accertamento di gravi delitti. Permane comunque il dubbio, come si è detto in dottrina[32], circa il compimento di alcune operazioni, strumentali alla captazione[33], compiute senza che i provvedimenti del pubblico ministero e del giudice per le indagini preliminari facciano alcun riferimento alle modalità pratiche di collocazione di microfoni e degli altri apparecchi captativi all'interno del domicilio e di altri luoghi di privata dimora.

La struttura del reato: a)condotta di indiscrezione

Il delitto in esame è stato introdotto con la L. n.98 del 1974 "Tutela della riservatezza e della libertà e segretezza delle comunicazioni", a seguito di una conclamata[34] insufficienza normativa del codice Rocco per l'inviolabilità del domicilio, dal momento che l'art. 614 tutelava la riservatezza domiciliare solo nei casi di introduzione o intrattenimento. Il reato, invece, è composto da due distinte fattispecie: la prima è caratterizzata da condotte di semplice indiscrezione, la seconda dalla rivelazione o diffusione di notizie o immagini, entrambe nei luoghi dell'art. 614.

La prima fattispecie consiste nella condotta di indebito procacciamento di notizie o immagini attinenti alla vita privata che avvengono nel domicilio altrui, ottenute mediante l'uso di strumenti di ripresa visiva o sonora da parte

[31] Così si è pronunciata la sez. VI, 31 gennaio 2011 n.11.
[32] FUMU G., *L'intercettazione di conversazioni domiciliari nella giurisprudenza di legittimità,* in *Studi sul processo penale in ricordo di Assunta Mazzarra,* CEDAM, Padova, 1996, pag. 192.
[33] Si pensi all'introduzione nel domicilio di falsi dipendenti delle aziende di servizi pubblici.
[34] Si veda, a titolo esemplificativo, MORSILLO G., *La tutela penale del diritto alla riservatezza*, Milano, 1966, Pag. 67.

La natura dell'oggetto del reato

di chiunque. Come è evidente, il reato è a forma vincolata, in quanto si richiede espressamente l'utilizzo di alcune tecniche di captazione, per questo motivo sono esclusi, quindi, dalla rilevanza penale, tutti i comportamenti di indiscrezione che non presentino quei caratteri che sono propri dei moderni strumenti di captazione del suono e dell'immagine[35]. Meno pacifico è il tema concernente gli oggetti configurabili nella categoria proposta dalla fattispecie. Vi è chi[36], infatti, ritiene che, in virtù del principio di uguaglianza, si possa operare una interpretazione estensiva, tale da non cadere nell'analogia, comprendendo anche gli strumenti tecnologici moderni e futuri poiché dotati di una inconfutabile penetrazione fraudolenta nella vita privata.

La giurisprudenza, invece, sin dal 1974 è stata sempre orientata ad una interpretazione letterale, come nel caso di chi scatti una fotografia dal cellulare all'insaputa o contro la volontà di chi ha uno *ius excludendi* nel luogo di lavoro [37] , escludendo invece casi quale l'installazione casalinga di un radiotelefono contenente una microspia[38].

"Indebitamente"

Ulteriore profilo interessante è quello concernente l'aggettivo "indebitamente" in riferimento alle modalità di captazione di immagini e suoni. Con esso sembrerebbe intendersi quell'attività che si svolga al di fuori di una qualsiasi situazione che la imponga o che eventualmente la giustifichi. La dottrina non è concorde: vi è chi ritiene che tale aggettivo sia indice di una antigiuridicità speciale [39] mentre per altri potrebbe trattarsi di un semplice riferimento all'assenza di cause di giustificazione. Sul tema invece, la giurisprudenza è convenuta sul fatto che, ad esempio, sarebbe da considerarsi indebita la

[35] A riguardo la dottrina è unanimemente concorde; si veda, per tutti, ANTOLISEI F., *Manuale di Diritto Penale – Parte speciale I,* Milano, Giuffrè Editore, 2003, pag. 243.
[36] Così fra i tanti PALAZZO F.C., *Considerazioni in tema di tutela della riservatezza (a proposito del nuovo art. 615 bis c.p.),* in *Rivista italiana di diritto e procedura penale*, 1975, pag. 130.
[37] Così, Sez. V, n. 10444 del 5 dicembre 2005.
[38] Il caso di specie, infatti, è stato ritenuto in grado di integrare l'art. 617: come ritenne Cass. Pen, Sez. II, 29.3.1988.
[39] Con questo termine si è soliti intendere il caso in cui, nel tenore letterale della norma, emergono parole o locuzioni come "abusivamente", "illecitamente", o altre simili. La dottrina, al riguardo, le considera come elementi costitutivi ulteriori della fattispecie, che sono individuabili al di fuori della specifica fattispecie penale, in altre normative, che delineano le linee di comportamento tali da poter, al di fuori di esse, dar vita a condotte illecite.

registrazione compiuta dal marito su conversazioni avvenute tra la moglie ed altri nell'abitazione comune, in quanto ciò che rileva ai fini del reato è, in ogni caso, la violazione della riservatezza domiciliare della persona offesa a nulla rilevando la disponibilità del domicilio da parte dell'autore della indebita intercettazione [40].

L'elemento soggettivo e l'errore

Infine, per quanto concerne l'elemento soggettivo, tale comma 1° richiede il dolo generico vale a dire la coscienza e volontà di procurarsi indebitamente, riprendendo notizie o immagini attenenti alla vita privata, queste ultime avvenute nei luoghi dell'art. 614. Interessante tuttavia il fatto che, a seconda della posizione che si assuma sul concetto dell'aggettivo "indebitamente", si avrà diversa applicazione di normativa penale per quanto riguarda l'errore.

Dovrà infatti, in linea di massima, richiamarsi la disciplina prevista dall'art. 47 c.p. sull'errore di fatto circa gli elementi costitutivi del reato; tuttavia potrebbe essere necessaria una disciplina differente sull'errore qualora "indebitezza" della interferenza realizzata, venga qualificata come generico richiamo all'assenza di cause di giustificazione o come elemento normativo della fattispecie integrante un caso di antigiuridicità speciale. Infatti, mentre, nel primo caso, l'errore non dovrebbe rilevare in quanto si tratterebbe di errore sulla legge penale (art. 5 c.p.) o tutt'al più rileverebbe ai sensi dell'art. 59 comma 4° c.p.[41], nella seconda si applicherà la disciplina prevista dall'art. 47, comma 3° c.p.[42] , in quanto si tratterebbe di errore su un elemento normativo del fatto.

b) condotte di rivelazione e diffusione

Venendo alla seconda fattispecie, presente al comma 2°, essa consiste, salvo non si configuri più grave reato, nella rivelazione o diffusione di notizie o immagini apprese nei luoghi dell'art. 614 con qualsiasi mezzo di comunicazione al pubblico. La distinzione fra rivelazione e diffusione non è mai stata limpida; talvolta si è ritenuto che con la rivelazione si intenda un

[40] Cass. Pen., Sez. V, n. 39827 dell' 8 novembre 2006.
[41] Cioè se il soggetto si è rappresentato per errore una situazione scriminante di fatto inesistente ma normativamente prevista.
[42] Portandosi dietro, tuttavia, i problemi relativi alla *interpretatio abragans* sul comma in questione.

concetto di divulgazione più limitato che non si attua tramite i mezzi tipici di pubblica informazione [43] . In dottrina, infatti, si contrappongono due orientamenti: secondo il primo le due condotte indicherebbero diversi modi di realizzazione del reato, mentre per il secondo, in virtù di un interpretazione logico-sistematica, si ritiene che siano semplicemente due diverse modalità di comunicazione per cui i due termini rileverebbero come sinonimi [44] . Probabilmente, la seconda soluzione si pone come la più convincente, in quanto sembra andare d'accordo con la *ratio* alla base di tale delitto, consistente nella tutela del diritto alla riservatezza domiciliare che risulterà egualmente offeso sia da condotte di rivelazione che di diffusione. In effetti, a voler forzatamente dare significati ontologicamente diversi alle due condotte, si potrebbe dover fronteggiare un irragionevole violazione del principio di eguaglianza in quanto, conseguendo una diversa capacità offensiva, sarebbero punite con la stessa pena. Conseguentemente, nel caso concreto, la soluzione migliore sarà quella di lasciar valutare al giudice circa la loro maggiore o minore gravità offensiva, mediante una diversa graduazione della pena consentita dall'ampia cornice edittale della fattispecie in esame[45].

Il rapporto con la fattispecie del comma 1°

Problema ben più grave è invece quello che investe la prodromicità di questa seconda fattispecie rispetto alla prima, chiedendosi quindi se la condotta di rivelazione o diffusione debba necessariamente prevedere una previa attività indebita di collettamento di notizie o immagini, propria del comma 1°[46]; il dubbio nasce dalla imperfetta dizione utilizzata al comma 2° che menziona "*le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo,"* come a voler dire che la prima condotta sia ontologicamente necessaria alla seconda. La maggior parte della dottrina, confortata da alcune

[43] PALAZZO F.C., *Considerazioni in tema di tutela della riservatezza (a proposito del nuovo art. 615 bis c.p.),* in *Rivista italiana di diritto e procedura penale*, 1975, pag. 149.
[44] Tra i primi abbiamo Antolisei, Manzini e Monaco; fra i secondi si ricordano Palazzo e Mantovani.
[45] Come peraltro ha sostenuto MONACO L., *Sub art. 615 bis c.p.*, in *Commentario breve al codice penale,* a cura di CRESPI, STELLA, ZACCALA', 4° Ed., Padova, 2003, pag. 1878.
[46] Spiegandolo con un esempio, è sufficiente che Tizio diffonda a molti le foto con l'amante dell'amico Caio dopo essersi trovato sul suo cellulare una foto scattata da Mevio (a cui aveva prestato il telefono per una chiamata), oppure Tizio stesso dovrà aver prima effettuato lo scatto col cellulare con coscienza e volontà?

decisioni in giurisprudenza, accoglie la tesi per cui la fattispecie di divulgazione e diffusone debba essere punita indipendentemente dalla rilevanza penale della condotta di indiscrezione [47] (quindi ad esempio mancanza di dolo o consenso del titolare del diritto alla riservatezza domiciliare), ciò in ragione del fatto che, privilegiando l'offensività della condotta di diffusione di notizie o immagini attinenti alla vita privata rispetto alla rimproverabilità del soggetto che effettua la condotta di indiscrezione, si fornisce una risposta migliore all'istanze di ampia tutela del diritto alla riservatezza personale già sacrificate da un scelta di incriminazione dei soli fatti invasivi della privacy domiciliare[48].

Anche in questa seconda fattispecie è richiesto il dolo generico, ovvero la coscienza e la volontà di rivelare o diffondere notizie o immagini della vita privata acquisite con l'uso di strumenti di ripresa visiva o sonora nell'altrui domicilio.

Ulteriori figure criminose

Inoltre, come nel caso della violazione di domicilio, è previsto che se i fatti siano commessi da un pubblico ufficiale o da un incaricato di pubblico servizio con violazione dei doveri o con abuso dei poteri inerenti all'ufficio o servizio, ovvero da chi eserciti la professione di investigatore privato, ricorreranno tre ulteriori distinte figure criminose. La prevalente dottrina sull'argomento ritiene che, in virtù della differenza sul soggetto attivo, tali figure rappresentino figure autonome di reato mentre solo una parte minoritaria le concepisce come circostanze aggravanti speciali. Come nel caso dei commi 1° e 2°, anche queste ulteriori fattispecie saranno punibili a titolo di dolo generico con l'aggiunta, rispetto alle altre, della consapevolezza della qualifica rivestita e dell'abuso commesso.

---

[47] Fra i tanti si cita MAZZA' P., *Considerazioni sul reato di divulgazione di notizie ed immagini attinenti alla vita privata,* in *Giurisprudenza di merito*, 1984, pag. 743.

[48] Per quanto concerne, invece, la giurisprudenza recente, si è ritenuto perfezionato il reato di illecite interferenze nel caso di un ufficiale di polizia giudiziaria che aveva consentito ai giornalisti di introdursi e filmare l'abitazione di un soggetto nei cui confronti era stata eseguita una misura cautelare contravvenendo agli ordini superiori che autorizzavano le sole riprese esterne: Cass. Pen., Sez. V, del 27 novembre 2008 n. 46509.

Prospettive di riforma in dottrina

A conclusione della trattazione di questo reato, si segnalano alcune critiche provenienti dalla dottrina. La tecnica di codificazione adottata, infatti, pur nel suo apprezzabile ancoraggio a situazioni o possibilità di aggressione del bene della riservatezza che, al tempo della sua elaborazione, si presentavano al legislatore come uniche modalità di offesa di tale bene, oggi ne costituisce una corazza, ciò infatti impedisce alla norma di adattarsi alle esigenze di tutela di un bene che non è più limitato ai soli luoghi di privata dimora. La riservatezza, si è visto, ha avuto negli anni una rilevante dilatazione dei suoi contenuti, specie in relazione all'evoluzione degli stessi diritti della personalità così come costituzionalmente protetti, ecco perché c'è chi afferma che *"l'art. 615 bis, pertanto, si appalesa inadeguato rispetto ad esigenze di tutela che scaturiscono dalle disposizioni costituzionali e dalla Convenzione europea, che pongono la libertà e la segretezza della comunicazione interpersonale al centro del sistema dei diritti* fondamentali"[49].

Fra le proposte più rilevanti, per una riflessione sulla necessità di rivisitazione del complesso delle disposizioni penali a tutela della vita privata ricordiamo chi, come Palazzo e Ronco, auspica un intervento sulla norma, tale da attribuire rilevanza alle condotte di illecita interferenza fraudolentemente realizzate anche fuori dalla sfera di esclusività spaziale della persona, purché espressive di una violazione del diritto del singolo alla riservatezza delle vicende della sua vita privata, o anche chi, ritenendo riduttiva l'analitica elencazione degli strumenti indicati dalla norma, propone la possibilità, attraverso un intervento riformatore, di un ricorso generico a tutti gli strumenti idonei a penetrarvi.

[49] RONCO M., *Vita privata (interferenze illecite nella)*, in *Novis, Digesto It.*,VII, UTET, Torino, 1987, pag. 163.

2.1 Reati informatici: accesso abusivo ad un sistema informatico o telematico: premessa (art. 615 ter)

Sviluppi storici

Il delitto di accesso abusivo ad un sistema informatico o telematico[50] fa parte di quel gruppo di reati introdotti nella prima metà degli anni novanta a seguito dello sviluppo di tecnologie informatiche e telematiche con le quali, connaturatamente, nasce anche il bisogno di garantire un adeguato livello di tutela. Questa disciplina, conosciuta anche col nome di *computer crimes*, rappresenta tuttora una materia altamente dibattuta, per la sua intrinseca difficoltà non solo tecnica, ma anche giuridica di delimitazione di concetti che siano poi traducibili all'interno del nostro panorama legale[51].

Il nostro legislatore, su spinta delle raccomandazioni del Consiglio d'Europa il quale richiedeva una uniformità legislativa europea sul tema, è intervenuto con la legge n. 547 del 23 dicembre 1993, in materia di criminalità informatica. Questa legge raccoglie quasi tutte le forme di aggressione informatica individuate dal Consiglio d'Europa nella raccomandazione "*sur la criminalità en relation avec l'ordinateur"* del 1989 n. 89. Tale documento è riconosciuto come punto di riferimento internazionale in materia; esso ripartisce i reati

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

[51] Si pensi ad esempio, come si approfondirà più avanti, alla figura dell'*hacker*, vale a dire colui che grazie alle sue particolari conoscenze informatiche è in grado di introdursi attraverso le reti in banche dati scavalcando misure di protezione fornite dal titolare del sistema.

L'origine comunitaria

informatici in due gruppi, un primo, detto "lista minima", comprende quelle fattispecie la cui incriminazione, per la loro diffusione e gravità, è ritenuta assolutamente necessaria, mentre il secondo, definito lista facoltativa, comprende quelle condotte da incriminare secondo la discrezionalità del Paese[52]. Questa legge fu la prima a fornire esplicitamente una tutela penale contro l'accesso abusivo ai sistemi informatici, nonostante in passato vi furono tentativi giurisprudenziali e dottrinali, seppur infelici[53], atti a offrire una tutela contro le intrusioni informatiche tramite l'applicazione allargata del già analizzato art. 614. Il nostro legislatore ha ritenuto che le condotte proprie dei *computer crimes* fossero delle nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, verso beni giuridici già presenti all'interno del codice penale; per questo motivo ha escluso la necessità di configurare un nuovo titolo specifico ed ha seguito la tecnica della cd. integrazione evolutiva, sviluppandoli accanto a quegli ulteriori reati che, dal punto di vista dell'interesse tutelato, risultassero più vicini. Infatti, come si evince dalla relazione al disegno di legge n. 2773 della rispettiva legge, si afferma che i sistemi informatici non sono altro che "*un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 Cost e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli artt. 614 e 615 c.p.*". Conseguentemente, il reato che ci accingiamo ad analizzare viene delineato come una forma moderna di aggressione alla libertà individuale e, per questo motivo, collocato nel titolo XII "Dei delitti contro la persona". Il legislatore, quindi, ha ritenuto che tali condotte fossero idonee ad incidere sulla sfera privata del singolo, legata al riconoscimento del diritto inviolabile della libertà individuale *ex* art. 2 Cost, di cui è specificazione il diritto alla riservatezza.

---

[52] Si veda, sul tema, PECORELLA G., *Il diritto penale dell'informatica*, Padova, 2000, pag. 8 e anche PICA G., *Diritto penale delle tecnologie informatiche*, UTET, 1999, pag. 14.

[53] In quanto, come è ovvio, immediatamente furono tacciati di analogia e forzature elevate del principio di legalità. Di fatti, CORRIAS LUCENTE, *Informatica e diritto penale: elementi per una comparazione con il diritto statunitense*, in *Diritto dell'informazione e dell'informatica*, 1987, Ia parte, pag. 195, fu tra quelli che invece richiesero un intervento ampliativo del legislatore.

2.1.1 Il dibattito sul bene giuridico tutelato

L' individuazione del bene giuridico tutelato dall'articolo 615 ter è argomento altamente dibattuto in dottrina, considerando anche la collocazione sistematica dell'illecito all'interno del Codice Penale, la quale ha sollecitato l'interrogativo, in particolare nelle prime fasi del dibattito, se questa fattispecie tuteli il bene giuridico comune alle norme che garantiscono la libertà domiciliare, oppure se sia possibile registrare l'emersione di un nuovo bene giuridico[54]. Da questo angolo visuale, la stessa dottrina ha parlato della tutela del cd. domicilio informatico, inteso come "*una espansione ideale dell'area di rispetto pertinente al soggetto interessato e volto a garantire il diritto di esplicare liberamente qualsiasi attività lecita all'interno*"[55]. Di conseguenza, nel dettaglio, si ritiene che al domicilio informatico si estenda lo *ius excludendi* del titolare che è proprio *in primis* del domicilio fisico, ragion per cui l'operatività della tutela penale va individuata a seconda della *voluntas excludendi* del titolare che, a seconda dei casi, tenderà a variare. Si vede dunque come, precisamente, il domicilio informatico, più che un nuovo interesse tutelato, rappresenti piuttosto una specificazione del domicilio tradizionale, imposta dalla natura dei luoghi informatici, con i quali ormai quotidianamente il singolo deve confrontarsi. È quindi evidente come, riprendendo le considerazioni effettuate circa il domicilio tradizionale e l'art. 14 Cost, col domicilio informatico si mira a tutelare ancora la libertà personale del singolo e, conseguentemente, anche la sua privatezza; non a caso, pienamente calzante risulta la posizione di Borruso che ritiene come tale fattispecie raccolga pienamente *"il valore acquisito dal computer per l'uomo di oggi: una sorta di propaggine della propria mente e di tutte le conoscenze, i*

Il domicilio informatico in dottrina…

[54] Di questo avviso è infatti PICA G., *Diritto penale delle tecnologie informatiche*, UTET, Torino, 1999, pag. 38.

[55] Questa la posizione di PICA, ma molti altri ne hanno condiviso i lineamenti essenziali, fra cui MONACO L., *Sub art. 615 bis c.p.*, in *Commentario breve al codice penale*, a cura di AA.VV., 4° Ed., Padova, 2003, pag. 1726; BORRUSO R., *La tutela del documento e dei dati*, *in Profili penali dell'informatica,* Milano, 1994, pag. 28; ALMA M., PERRONI C., *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Diritto penale e processo*, 1997, pag. 505.

ricordi, i segreti che essa custodisce". Per questo motivo non importano più di tanto la natura od il contenuto dei dati inseriti nel sistema informatico, poiché la tutela è innanzitutto indirizzata alla sfera stessa che li contiene, dando vita ad una tutela particolarmente ampia ed onnicomprensiva.

… e in giurisprudenza

Inoltre, la tesi del domicilio informatico è apprezzata anche dalla giurisprudenza di legittimità che, nella sua prima pronuncia sul tema, afferma che l'articolo in questione, tutelando i sistemi informatici e telematici, non mira solo a garantire la riservatezza delle informazioni ivi contenute, bensì l'intera sfera della personalità del titolare, comprendendo anche i diritti economico-patrimoniali [56] , intendendo dire così che è al suo interno ricompreso uno *ius excludendi* qualunque sia il contenuto dei dati racchiusi all'interno del sistema, fin quando sia attinente alla propria sfera di pensiero o comunque alla propria attività. A motivazione di ciò, la Corte rammenta la lettera e la *ratio* della norma, poiché non opera distinzioni di sistemi a seconda dei contenuti, richiede soltanto che si tratti di sistemi protetti da misure di sicurezza. Tra l'altro, limitare eventualmente l'ambito di operatività a seconda del contenuto dei dati, comporterebbe una mancata tutela di alcuni contenuti come quelli relativi ai profili economico-patrimoniali[57]. Di conseguenza, è bene ripeterlo, la Cassazione ritiene che il domicilio informatico rappresenti un luogo fisico in cui sono contenuti dati di qualsivoglia natura salvaguardati contro ogni tipo di intrusione, indipendentemente dai fini che muovono il soggetto attivo del reato.

Ecco quindi che, come essa ha anche ribadito a distanza di pochi mesi, l'articolo 615 ter tutela non solo il diritto alla riservatezza del titolare, ma anche, più generalmente, il suo diritto di escludere, con riguardo a ciò che il legislatore delinea come suo domicilio informatico.

---

[56] Si tratta della sentenza di Cassazione, Sez. VI del 4 novembre 1999 n.3067.

[57] Si pensi alle banche dati protette da misure di sicurezza accessibili dietro pagamento di uno specifico canone: ciò significherebbe non fornire tutela ai diritti di enti e persone giuridiche, non perché a tali categorie soggettive non siano estensibili i diritti della personalità ed in particolare della riservatezza, ma perché fra dette categorie vi sono soggetti titolari di sistemi informatici protetti da misure di sicurezza (enti pubblici, società commerciali) per i quali lo *ius excludendi* è strettamente correlato a diritti di natura economico-patrimoniale.

A questo punto, come anche è stato ribadito negli anni a venire [58], probabilmente la posizione dottrinaria che vede, nel domicilio informatico, una sola specificazione del domicilio fisico non è sufficientemente convincente. Al contrario gli si deve riconoscere *"dignità di un vero e proprio nuovo bene giuridico, che può indicarsi come riservatezza informatica e che, in concreto, si risolve nella tutela dell'indisturbata fruizione del sistema informatico o telematico, cosicché è configurabile la sussistenza del reato a prescindere dal contenuto - di natura personale o meno - dei dati racchiusi nel sistema informatico violato"*[59].

La dottrina contraria: lo schema proprietario

Tuttavia, altra parte della dottrina[60] rigetta il concetto di domicilio informatico, in ragion del fatto che comporta una dilatazione esagerata della tutela penale, ritenendo difficilmente realizzabile una nozione unitaria di domicilio che raccolga tanto i luoghi indicati dall'art. 615 quanto i sistemi informatici e telematici del presente articolo. Si è detto che vincolare ad un determinato ambito spaziale la tutela penale predisposta con la previsione dei delitti informatici significa *"svuotare di significato e utilità"*[61] l'introduzione delle dette previsioni. Quest'altra porzione di dottrina, conclude affermando che il computer "*non ha nulla in comune con i diversi ambiti spaziali nei quali la persona può liberamente estrinsecarsi, che entrano a far parte della nozione di domicilio, presentando piuttosto notevoli affinità con il tradizionale*

[58] Si veda la ss. Trib. Rovereto, 2 dicembre 2003 n. 343.
[59] Così FLOR, a nota di *Dir. Pen. e Processo*, 2005, 1, pag. 81 a commento della sentenza sovracitata. Inoltre, casi che raccolgono concreti esempi di profili anche economico-patrimoniali non sono mancati nel tempo: con sentenza di Cassazione n.11689 del 2007 si è ritenuto integrato tale delitto nella introduzione in una centrale Telecom e nell'utilizzo di apparecchi telefonici, modificati all'uopo, per allacciarsi a numerose linee di utenti, a loro insaputa stabilendo contatti con utenze caratterizzate dal codice 89; si è ritenuto integrato il reato anche con la condotta di chi, in concorso con il titolare di un esercizio commerciale, utilizzi sul terminale POS in dotazione di quest'ultimo una carta di credito contraffatta perché, sebbene il titolare dell'esercizio commerciale sia legittimato a utilizzare il terminale POS, l'accesso effettuato con utilizzo di una chiave contraffatta assume carattere abusivo (C., Sez. V, n.44362/2003).
[60] Tra i quali, su tutti, ANTOLISEI F., *Manuale di Diritto Penale – Parte speciale I,* Milano, Giuffrè Editore, 2003, pag.235.
[61] PAZIENZA P., *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547*, in *Rivista italiana di diritto e procedura penale*, 1995, pag. 750.

cassetto, che per anni ha svolto e in gran parte continua ancora oggi a svolgere la stessa funzione dei più moderni elaboratori"[62] .

Conseguentemente, in dottrina, si è fatta strada una ulteriore concezione alternativa alla tesi del domicilio informatico in ragion del fatto che, per questo orientamento[63], i sistemi informatici non possono essere assimilati ai luoghi privati riconducibili alla nozione di domicilio rilevante ex art. 614, in quanto i contenuti del sistema informatico non sempre presenterebbero carattere strettamente personale. Questa posizione ritiene che, riconducendo sotto il comune denominatore dello schema proprietario, inteso come signoria sulla *res*, il bene protetto dall'articolo 615 ter e quello di cui all'art. 637[64], la norma in esame tuteli l'indisturbata fruizione del sistema informatico analogamente alla tutela offerta dall'art. 637 che, nel reprimere l'ingresso abusivo nel fondo altrui, protegge da ogni possibile turbativa la proprietà fondiaria. Tuttavia, come è facilmente immaginabile, una posizione di questo tipo è stata fortemente contestata, a partire dalla diversità degli interessi tutelati delle due norme (una tutela patrimonialmente la proprietà fondiaria, l'altra la privacy) sino alla evidente differenza di pena che ricorre fra i due reati.

La tesi dell'integrità del sistema

Ulteriore posizione[65], sempre alternativa a quella del domicilio informatico, ritiene che l'interesse tutelato dalla norma in esame sia l'integrità del sistema, dei dati e dei programmi in esso contenuti. Tuttavia, anche tale orientamento non è pacificamente accolto in dottrina; si è infatti affermato che esso non coglie la vera funzione della norma in esame, sottolineandone invece aspetti secondari, poiché così ricostruito il reato di accesso abusivo mirerebbe più che altro a prevenire una conseguenza di esso, vale a dire la causazione di un

[62] PECORELLA C., *Il diritto penale dell'informatica*, Padova, 2a ed., 2006, pag. 316.
[63] Fra cui ROSSI-VANNINI, *La criminalità informatica: le tipologie di computer crimes di cui alla L. 547/1993 dirette alla tutela della riservatezza e del segreto*, in *Rivista trimestrale di diritto penale dell'economia*, 1994, pag. 427.
[64] Rubricato ingresso abusivo sul fondo altrui, punisce chiunque senza necessità entra nel fondo altrui recinto da fosso, da siepe viva o da un altro stabile riparo.
[65] PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, pag. 70.

danno al sistema o alle sue componenti, che risulterebbe avere un rilievo episodico o secondario rispetto all'obiettivo primario costituito dall'acquisizione di informazioni in senso lato riservate. Inoltre l'attribuzione di una tale funzione al reato in esame comporterebbe anche un accavallamento con ulteriori fattispecie volte a tutelare l'integrità dei sistemi informatici, come il delitto di danneggiamento di sistemi informatici o telematici (art. 635 bis), il delitto di attentato a impianti di pubblica utilità (art. 420), la diffusione di programmi virus (art. 615 quinquies)[66]. Quindi, accettando una tale chiave di lettura, risulterebbe irragionevole la delimitazione della tutela predisposta dall'art. 615 ter ai soli sistemi informatici protetti da misure di sicurezza, posto che l'interesse alla integrità dei dati ed alla loro piena utilizzabilità sussiste certamente per tutti i titolari dei detti sistemi, indipendentemente dalla predisposizione di tali misure.

La tesi della "sola" riservatezza

Infine, una ulteriore tesi, per quanto concerne il bene giuridico tutelato dalla presente fattispecie, è quella che cerca di superare le ambiguità e le incertezze che caratterizzano la nozione di domicilio ora affrontate; essa[67] ritiene che l'intervento della sanzione penale sia giustificato solo "*dalla tutela del contenuto dei dati e non del contenente*", cosicché il bene giuridico protetto dalla disposizione in esame viene individuato nella riservatezza dei dati e dei programmi contenuti in un sistema informatico, messa in pericolo dalle intrusioni di terzi non autorizzati per la facilità con cui è possibile procurarsi dati e programmi in brevissimo tempo una volta superate le barriere poste a protezione del sistema. In questo caso, di conseguenza, la fattispecie si configurerebbe necessariamente come di pericolo astratto; inoltre, si potrebbe dire che il reato non sussisterebbe quando oggetto della violazione sia un sistema che, sebbene protetto da misure di sicurezza, non contenga alcun dato

[66] Tali critiche sono mosse principalmente da PECORELLA C., *Il diritto penale dell'informatica*, Padova, 2a ed., 2006, pag. 321 e ss.

[67] MANTOVANI F., *Diritto Penale – Parte Speciale, delitti contro la persona,* Padova, 2012, pag. 545; POMANTE G., *Internet e criminalità*, Giappichelli, Torino, 1999, pag. 26; CUOMO-IZZI, *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico*, in *Cassazione Penale*, 2002, pag. 1021.

o programma oppure contenga informazioni di completo dominio pubblico, reperibili da chiunque; ciò in ragione della ovvia inoffensività del fatto, qualora si accettasse come bene giuridico tutelato la sola riservatezza dei dati, senza accogliere anche le considerazioni di cui *supra* sul domicilio informatico. Accogliendo questa soluzione ermeneutica si ritiene sia possibile attribuire un significato coerente al requisito della protezione del sistema mediante misure di sicurezza, nel senso che la tutela penale non opererebbe in modo indiscriminato, ma si rivolgerebbe esclusivamente a quei dati e programmi alla cui riservatezza il "titolare" abbia mostrato interesse, avendo predisposto delle barriere di protezione contro le eventuali intrusioni altrui[68].

A conclusione di questo insieme di posizioni ermeneutiche sul bene giuridico tutelato, preme tuttavia ricordare come, nonostante tutto, la posizione della Corte di Cassazione, che ancora accoglie il concetto di domicilio informatico, sia la più acclamata fra dottrina e giurisprudenza, in quanto maggiormente incline a coniugarsi col dettato normativo in esame; di conseguenza, l'analisi della fattispecie verrà impostata sulla base di quest'ultima considerazione, ma riportando comunque gli orientamenti dottrinari minoritari che, a seconda del bene giuridico inteso, si articolano differentemente.

[68] Tuttavia non è mancata una voce contraria in dottrina per cui *"un notevole rischio può discendere anche dalla violazione di un sistema attualmente vuoto, sia perché comporta comunque l'apprensione di tale informazione, sia perché può costituire il mezzo per favorire successivi abusi"*. Così CORRIAS LUCENTE, *I reati di accesso abusivo e danneggiamento informatico*, Relazione al seminario su I reati informatici, Roma, consultato 15-16.08.2014, in http://www.giustizia.it/

2.1.2 La struttura del reato

Reato di danno, pericolo, o astratto?

Il reato di accesso abusivo ad un sistema informatico o telematico, qualora si accolga l'orientamento che afferma il parallelismo fra la seguente fattispecie e quella di violazione di domicilio, è un reato di danno. Dunque, al di là del fatto che nel sistema siano presenti dati o programmi di qualsiasi natura, la lesione dell'interesse tutelato avviene a prescindere, in quanto ciò che risulta leso è la privacy informatica, così come nell'art. 614 è lesa la privatezza materiale del soggetto passivo, senza che rilevi a nulla il fatto che il domicilio sia un'abitazione a regola d'arte o semplicemente un edificio abbandonato sfruttato occasionalmente quale dimora. Di conseguenza, sempre parallelamente, come nel reato di violazione di domicilio non si richiedono sofisticati impianti antiintrusione, così nel reato in esame non è necessaria la predisposizione di misure di sicurezza altamente complesse, essendo sufficiente la semplice esistenza delle stesse in quanto tali da costituire espressione inevocabile della volontà del titolare di esercitare uno *ius excludendi*[69].Nonostante queste considerazioni, permane tuttavia chi[70], sempre all'interno della tesi della tutela del domicilio informatico, rintracci, tramite una interpretazione della condotta tipica, un reato di pericolo. Si ritiene, infatti, che sussista il pericolo che l'agente possa carpire quante più informazioni possibili semplicemente entrando all'interno della memoria del computer *invito domino.* Qualora invece si accolga la posizione di chi sostiene che tale fattispecie sia posta a tutela della sola riservatezza dei dati contenuti nel sistemi, o della integrità dei dati e dei programmi, essa si configurerebbe quale reato di pericolo astratto.

---

[69] Molto chiaro ad esporre tale concetto è LUSITANO D., *In tema di accesso abusivo a sistemi informatici o telematici,* in *Giurisprudenza Italiana,* 1998, pag. 1924 per cui "*dato che il principio sotteso a tale reato è la tutela della libertà, sotto l'aspetto del divieto di intromissioni, di interferenze, turbative della sfera privata di un soggetto, che avvengano contro la volontà dello stesso, detta tutela opera indipendentemente dalla importanza dei dispositivi di sicurezza, dalla natura dei dati contenuti e finanche dalla esistenza degli stessi dati".*

[70] BORRUSO R., *La tutela del documento e dei dati*, *in Profili penali dell'informatica,* Milano, 1994, pag.28 e ss.

2.1.3 Il significato di «sistema informatico e telematico protetto da misure di sicurezza»

Tale norma richiede, come requisito, la presenza di alcuni sistemi, definiti come informatici o telematici, propri di questi nuovi reati connaturati nello scenario tecnologico degli ultimi vent'anni.

Il sistema informatico

Il sistema informatico indica quel complesso organico di elementi fisici (*hardware*) ed astratti (*software*) che compongono un apparato di elaborazione dati[71].

In giurisprudenza[72] si è definito "*come una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche in parte, 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, effettuata attraverso simboli (bit), in combinazioni 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"*.

Dunque, come si evince da questa dettagliata proposizione dei giudici di legittimità, non può rientrare in un sistema informatico tutto ciò che, in un sito web o nel mondo dell'informatica, non è capace di gestire od elaborare dati in vista dello svolgimento di una specifica funzione[73].

Il sistema telematico

Per quanto concerne il sistema telematico, in virtù di una concezione di tipo estensivo, con esso si intende ogni altra forma di telecomunicazione che

[71] La definizione ufficiale, fornita dall'art. 1 della Convenzione di Budapest del 2001 sul Cybercrime, ratificata in Italia con legge n.48 del 2008, è la seguente: "*è sistema informatico qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati"*.

[72] Tra le quali si ricorda *in primis* la sentenza di Cassazione del 4 ottobre 1999 n.3067 ed in seguito la sentenza di Cassazione n.36721 del 2008.

[73] Di fatti si è escluso il reato nel caso di riproduzione di dati di una banca dati contenuta in un sito non protetto da alcun sistema di sicurezza e in relazione al quale non risulta essersi verificata alcuna intrusione (Trib. Milano Sez. III Sent., 19/03/2007).

fruisca dell'apporto informatico per essere gestito oppure che sia al servizio di tecnologie informatiche, indipendentemente dal fatto che la comunicazione avvenga via cavo, etere o altro[74]. Vi è, inoltre, chi ritiene che l'espressione in esame, nonostante l'espressa dizione legislativa, sia ricompresa nella più generale categoria di sistema informatico[75].

Considerazioni dottrinali e giurisprudenziali sui sistemi

Analizzando ambedue nello specifico, è pacifico che non sia necessario un elevato grado di complessità del sistema, superiore a quello di un normale *personal computer*, di conseguenza, anche questi ultimi possono essere ricondotti nelle nozioni di sistema ora analizzati in quanto sono indubbiamente in grado di contenere un patrimonio ingente di dati e informazioni che non può essere escluso dalla protezione penale[76]. Tuttavia, alcuni tendono ad estromettere dalla tutela dell'articolo 615 ter i sistemi informatici predisposti esclusivamente alla gestione e al controllo del funzionamento di apparecchi che erogano beni e servizi, in quanto, in questi casi, "*l'accesso abusivo è strumentale al conseguimento di beni o servizi senza il pagamento del corrispettivo e, pertanto, assume rilevanza solo ove sia penalmente sanzionato anche l'uso non autorizzato di un sistema informatico oppure il conseguimento fraudolento delle sue prestazioni"*[77]. Opposta è la posizione dei giudici di legittimità per cui, come si è giù avuto modo di vedere, in generale, la norma in esame, tutelando lo *ius excludendi,* ben comprende anche i diritti economico-patrimoniali ad esso connaturati[78].

---

[74] A questa posizione se ne oppone un'altra, in vero minoritaria, per la quale è sistema telematico solo quello che avviene tramite forme di comunicazione tra più computer via linea telefonica. Come è ovvio però, si andrebbe cosi ad escludere dalla tutela penale alcuni aspetti di utilizzazione delle tecnologie informatiche in cui si è comunque in presenza di comunicazioni gestite e coordinate da tecnologie informatiche come le interconnessioni via etere fra sistemi video: BUONOMO G., *Metodologia e disciplina delle indagini informatiche*, in BORRUSO-BUONOMO-CORASANITI-D'AIETTI, *Profili penali dell'informatica*, Giuffrè, Milano, 1994, pag. 148.

[75] PECORELLA G., *sub. Art. 392*, in MARINUCCI-DOLCINI, *Codice penale commentato,* IPSOA, Milano, 2011, pag. 5981.

[76] CORRIAS LUCENTE, *I reati di accesso abusivo e danneggiamento informatico*, Relazione al seminario su I reati informatici, Roma, 19.07.2014, in http://www.giustizia.it/

[77] PECORELLA G., *cit*., 5981.

[78] In questo senso, è stato qualificato sistema informatico qualsiasi servizio televisivo o telefonico che si avvalga delle tecnologie informatiche, ricomprendendo così nella tutela della norma anche le linee telefoniche poiché esse si avvalgono di sistemi di trasmissione delle comunicazioni attuate con la codificazione di segnali in forma di flusso continuo di cifre (*bit*) caratterizzate inoltre nel loro

Le misure di sicurezza: traduzione oggettiva della volontà del titolare?

Come si evince dalla dizione normativa, i sistemi in questione devono essere solo quelli protetti da misure di sicurezza, con le quali si intendono quei dispositivi idonei ad impedire l'accesso al sistema a chi non sia autorizzato. Come si è accennato *supra,* è sufficiente che tali dispositivi abbiano una disposizione di sicurezza anche minima e facilmente raggirabile, poiché la sola esistenza di essa implica che l'accesso è consentito in ogni caso ad un numero determinato di persone, ponendo per le altre un divieto d'accesso[79]. Detto ciò, è facile riconoscere come, nelle misure di sicurezza, sia rinvenibile il medesimo significato della scritta "vietato l'ingresso", che sia presente in una proprietà privata, in quanto è in grado, nonostante la evidente facilità di ignorarlo, di ingenerare in terzi la nozione di altruità della proprietà in questione.

Sulla stessa corrente di pensiero è, infatti, la prevalente giurisprudenza di legittimità, per la quale la semplice presenza di qualsiasi mezzo protettivo è di per sé stessa in grado di tradurre la precisa volontà dell'avente diritto di escludere intrusioni all'interno del sistema[80]. D'altronde, ragionando per assurdo, richiedere un livello di sicurezza fortemente elevato, sarebbe come richiedere, per l'art. 614, un ulteriore sistema impeditivo nei confronti di terzi al di là del semplice *ius excludendi* del titolare, che è presente nell'abitazione, restringendo eccessivamente l'area di tutela penale e strozzando all'inverosimile lo stesso principio di offensività[81]. Fatte tali considerazioni, ecco che appare chiaro come, in realtà, il significato della norma, come poi

---

trasporto in tale forma all'altro estremo, dove il segnale di origine è ricostruito e inoltrato nuovamente dopo essere stato registrato (Cass. pen. Sez. V, 02/07/1998, n. 4389).

[79] Si esprime così , D'AIETTI G., *Profili penali dell'informatica*, Giuffrè, Milano, 1994, pag. 72. Vi si contrappone chi ritiene che la dizione legislativa che parla di "misure di sicurezza" al plurale porta a ritenere che una semplice parola chiave o un codice d'accesso non integrano il requisito in parola, che dovrebbe essere inteso come qualcosa di più complesso di una semplice password: CECCACCI G., *Computer Crimes. La nuova disciplina dei reati informatici*, Giuffrè, Milano, 1994, pag.70.

[80] Su tutte si veda la sentenza di Cassazione n.36721 del 21 febbraio 2008.

[81] Fra i casi in cui si è escluso il reato, si ricorda quando l'agente, dipendente di una impresa, si limiti ad accedere, avvalendosi solo di dati e strumenti di cui sia legittimamente in possesso (dunque non "neutralizzando" illecitamente le misure di sicurezza), ad una parte del sistema comune a tutti i dipendenti dell'impresa, a nulla rilevando che, a causa della condotta illecita di terze persone che abbiano eventualmente neutralizzato le misure di sicurezza, in esso siano collocati anche dati riservati al titolare, che l'agente si sia limitato a visualizzare o duplicare (C., Sez. V, 4.12.2006, n. 6459).

sottolineato dalla Cassazione[82], non sia caratterizzato tanto dalla violazione dei sistemi protettivi, quanto dalla violazione delle disposizioni del titolare, come avviene nella violazione di domicilio, concretizzate nella contrarietà del soggetto attivo avverso lo *ius excludendi*. Conseguenza di ciò è che, eventualmente, non sarebbe necessaria la violazione della misura di sicurezza da parte del soggetto attivo ai fini della sussistenza del reato.

…oppure apparecchiatura a sé stante calibrata sui dati protetti?

Come è prevedibile, a questa posizione si contrappone una restrittiva dottrina, fra cui Pecorella, che sulla base dell'idea dell'interesse protetto posto a tutela dei sistemi informatici, ritiene che le misure di sicurezza debbano essere effettivamente scavalcate e, inoltre, siano di un livello proporzionato al genere di dati che vanno a tutelare. C'è da dire, tuttavia, che quest'orientamento manca del supporto della giurisprudenza di legittimità, essendo rinvenibile tutt'al più in sporadiche pronunce del giudice di merito[83].

Invece, riallargandoci alla prima posizione menzionata, le misure di sicurezza di cui alla norma in esame ricomprendono qualsivoglia accorgimento predisposto per impedire l'accesso al sistema e, quindi, anche le misure logiche e fisiche (es.: chiave metallica per l'accensione dell'elaboratore), o quelle poste a protezione dei locali (porte blindate, personale di vigilanza, ecc).

Questa posizione allargata[84] sembra la più condivisibile, in quanto pone in luce allo stesso tempo l'idea del bene giuridico tutelato del domicilio informatico che ben si sposa col titolo nel quale il reato è stato introdotto, ed il parallelismo del reato in esame con la fattispecie dell'art. 614. Fra l'altro, a

[82] C., Sez. V, 7.11.2000 n. 12732.

[83] In tal senso si è affermato che le misure di sicurezza non si limitano ad essere una manifestazione oggettiva della volontà dell'avente diritto, ma costituiscono un elemento costitutivo del reato che non sussiste laddove le misure siano inidonee alla tutela del sistema informatico (G.I.P. Roma 4.4.2000).

[84] Ed anche essa è, inoltre, supportata dalla giurisprudenza di legittimità: si è ritenuto che, ai fini della sussistenza del reato, assumono rilevanza non solo le protezioni interne al sistema informatico, come le chiavi di accesso, ma anche le protezioni esterne, come la custodia degli impianti, in particolare quando si tratti di banche dati private, per definizione interdette a coloro che sono estranei all'impresa che le gestisce. Conformemente di recente si precisa che la protezione del sistema può essere adottata anche con misure di carattere organizzativo, che disciplinino le modalità di accesso ai locali in cui il sistema è ubicato e indichino le persone abilitate al suo utilizzo (C., Sez. V, 8.7 - 1.10.2008, n. 37322).

sostegno di questa interpretazione, in dottrina si richiama la aggravante prevista nel comma 2°, espressamente riferita a colui che usa violenza sulle cose o alle persone ovvero a chi è palesemente armato, la quale appare in perfetta consonanza anche con l'ipotesi di un accesso fisico.

Inoltre, sempre sulla scia di questa posizione, nell'ipotesi di temporanea disattivazione di misure di sicurezza (per es. in corso di sostituzione, per manutenzione del sistema, aggiornamento del software) per taluni il reato non sussiste in quanto la locuzione del legislatore "protetto da misure di sicurezza" richiede l'attualità e l'efficacia della protezione; in realtà, invece, considerata la funzione delle misure di sicurezza preordinate a connotare i dati come riservati, l'accesso abusivo può verificarsi anche in caso di temporanea disattivazione, purché l'agente ne sia a conoscenza, non essendo necessario, ai fini della sussistenza del reato, la violazione delle misure di sicurezza mentre è, invece, necessario che nel sistema siano presenti dei dati o dei programmi e che questi non siano di pubblico dominio.

Conseguenza di questo discorso è che, se l'introduzione avviene in un sistema aperto[85], cioè non protetto, il fatto non costituisce il reato in esame, salva tuttavia la integrazione di un diverso reato (frode informatica ex art. 640 ter, o danneggiamento di sistemi informatici ex art. 635 bis) sussistendone i loro elementi strutturali.

[85] Tuttavia anche qui, *a contrario*, per alcuni, si è ritenuto che l'applicazione della tutela penale ai soli sistemi protetti da misure di sicurezza restringa irragionevolmente l'area del penalmente rilevante, escludendo ad esempio i casi in cui sia stata esplicitata la *voluntas excludendi* ma il sistema non sia stato dotato di misure di sicurezza, e dunque si reputa erroneo considerare dette misure come l'unica forma di dimostrazione possibile della *voluntas excludendi:* GALDIERI P., *L'introduzione contro la volontà del titolare fa scattare la responsabilità dell'hacker*, in *Guida al diritto*, 2001, pag. 44.

2.1.4 Le condotte rilevanti

La condotta rilevante nell'articolo in questione, tra l'altro costituita, in parte, da espressioni già utilizzate relativamente alla fattispecie di violazione del domicilio, consiste alternativamente nell'introdursi abusivamente in un sistema protetto ovvero nel permanervi *invito domino*, vale a dire nonostante l'esercizio, da parte del titolare, dello *ius excludendi*.

La condotta dell'introduzione abusiva

Per quanto concerne la prima, un aspetto da analizzare è quello circa la necessità o meno di un collegamento "fisico" relativamente all'accesso (la semplice accensione di uno schermo) oppure se sia necessario un accesso logico, vale a dire il superamento delle barriere protettive del sistema che consentano poi l'avvio di dialogo con il *software*. Per la dottrina prevalente, l'accesso cd. virtuale richiede conseguentemente l'inizio di dialogo col *software* dal momento che, in concreto, un sistema informatico e telematico *"non è fisicamente penetrabile"*[86]. Nello specifico, si è poi ritenuto che la condotta di accesso può suddividersi in due eventuali fasi: l'accesso fisico, caratterizzato, ad esempio, dalla materiale accensione di un computer, e l'accesso logico, consistente nell'inizio di colloquio colla macchina. Da qui meglio si evince come, per perfezionare tale condotta, non è sufficiente il mero accesso fisico, ma sia necessaria una "introduzione elettronica" che avvii un dialogo con l'operatore informatico, a che possa in seguito avvenire uno scambio di dati.

Non manca, come di consueto, una posizione minoritaria[87] che, facendo leva sull'aggravante della violenza a cose e persone, ritiene che la condotta tipica possa essere integrata anche dall'ingresso abusivo di un soggetto semplicemente nei locali in cui sia custodito l'elaboratore.

Per quanto riguarda il momento consumativo del reato, vale a dire quando si ritiene conseguito l'accesso, esso coincide nell'attimo in cui si ha la possibilità

[86] D'AIETTI, *Profili penali dell'informatica*, Giuffrè, Milano, 1994, pag. 68.
[87] GIANNANTONIO E., *Manuale di diritto dell'informatica,* CEDAM, Padova, 1994, pag. 435.

di aprire liberamente uno qualsiasi dei documenti presenti nel sistema che risultano poi analizzabili su uno schermo oppure quando sono ormai assenti ostacoli da superare per arrivare a soddisfare lo scopo dell'intrusione informatica. A fronte dell'analisi compiuta circa l'interesse tutelato, può dirsi pacificamente[88] che non è necessaria, per il perfezionamento, la conoscenza dei dati e dei programmi memorizzati all'interno del sistema, dato che la soglia di punibilità è anticipata rispetto allo stadio della conoscenza, essendo sufficiente che l'agente si sia introdotto abusivamente nel sistema altrui.

Di conseguenza, un' introduzione di questo tipo rappresenta la realizzazione di quella situazione di pericolo nei confronti della segretezza di dati e programmi dell'elaboratore che la fattispecie penale in questione mira a tutelare.

Per quanto concerne la giurisprudenza, di recente[89] si è detto che il reato non richiede, come accennato, l'effettiva conoscenza da parte del soggetto attivo dei dati protetti, in quanto rileva semplicemente il prelievo indesiderato di tali dati. Inoltre, si è poi detto che integrerà la condotta tipica la duplicazione di dati acquisiti con accesso abusivo poiché *"siffatta sottrazione di dati non è altro che una forma di presa di conoscenza di notizie cui è preordinata l'intrusione che può risolversi sia in una semplice lettura che in una vera e propria copiatura dei dati rinvenuti nel sistema oggetto dell'introduzione".*

A contrario, certa giurisprudenza, accompagnata da dottrina[90] comunque minoritaria, ha rilevato che per l'accesso è necessaria la conoscenza dei dati o informazioni contenuti nel sistema, in quanto la sola introduzione, di per se stessa, non appare meritevole di criminalizzazione, non potendo costituire bene meritevole di tutela l'inviolabilità del sistema informatico e telematico in quanto tale.

---

[88] Così, fra i tanti, PECORELLA G., *Il diritto penale dell'informatica,* Padova, 2000, pag. 336 e anche PICA G., *Diritto penale delle tecnologie informatiche,* UTET, 1999, pag. 57.

[89] Corte d'Appello di Bologna, Sez. II, 30.1.2008.

[90] MARINI G., *Lineamenti del sistema penale*, Giappichelli, Milano, 2008, pag. 386. Tuttavia c'è anche chi, addirittura, ritiene che per integrare un'ipotesi di introduzione sia sufficiente il mero entrare in contatto con il sistema oppure qualsiasi tipo di interferenza, resa possibile dallo sviluppo tecnologico, nel programma o nella memoria di apparati informatici o telematici non aperti ma garantiti dall'adozione di mezzi di protezione: FONDAROLI C., *La tutela penale dei "beni informatici"*, in *Diritto dell'informazione e dell'informatica*, 1996, pag. 312.

Fra le più recenti sentenze della giurisprudenza di legittimità[91], si è invece affermato che integra il reato di accesso abusivo al sistema informatico la condotta di un pubblico dipendente impiegato presso l'Agenzia delle entrate che effettui interrogazioni sul sistema centrale dell'anagrafe tributaria sulla posizione di contribuenti non rientrante, in ragione del loro domicilio fiscale, nella competenza del proprio ufficio.

Una questione particolarmente analizzata è invece quella dei sistemi dotati di barriere protettive progressive atte a penetrare nel cuore del sistema oppure di barriere alternative a seconda degli archivi che si intenda consultare. Per alcuni non sembra necessario superare tutte le barriere né tantomeno "compiere" un percorso utile nel sistema che consenta di trarre dati o notizie, poiché sarebbe sufficiente che le procedure poste abbiano messo *"l'operatore in grado di muoversi in qualche modo, anche superficialmente"*[92]. La posizione opposta, condivisa da Barruso, sarebbe quella di ritenere integrato e non solo tentato il reato quando non vi siano più ostacoli da superare onde soddisfare lo scopo intrusivo.

In realtà, come detto, per risolvere questioni di tal tipo, bisognerà fare chiarezza sul bene giuridico tutelato, dal momento che, accettando come tale il domicilio informatico e considerando il reato come di pericolo astratto, anche condotte non completamente intrusive all'interno del sistema saranno tuttavia sufficienti ad integrarlo.

La condotta del mantenimento abusivo

Venendo ora alla seconda condotta, è punito il mantenersi in un sistema protetto contro la volontà, espresso o tacita, del titolare del diritto di escludere. Anche qui, il legislatore sanziona la mera permanenza del sistema e non eventuali attività poste in essere contestualmente, come l'effettiva presa di coscienza di dati o informazioni.

Per la dottrina dominante, tale ipotesi è integrata ogni volta in cui, a seguito di un' introduzione inizialmente autorizzata, o autorizzata in certi limiti modali, o

[91] In questo senso Corte di Cassazione, Sez. V., del 24 aprile 2013, n. 22024.

[92] Così LUSITANO D., *In tema di accesso abusivo a sistemi informatici o telematici*, in *Giurisprudenza Italiana*, 1998, pag. 1924.

causale, o involontaria, l'agente permanga poi nel sistema nonostante il dissenso del titolare dello *ius excludendi*, o comunque oltre i limiti consentiti. Come si vede, dunque, sebbene l'introduzione sia connaturatamente prodromica alla permanenza, tuttavia la distinta previsione di queste due condotte è utile proprio perché, a fronte di un' eventuale introduzione al sistema inizialmente lecita, questa può trasformarsi in un mantenimento illegittimo, oltrepassando , ad esempio, i limiti posti da una autorizzazione.

È interessante notare che, quando la permanenza nel sistema abbia come antecedente una introduzione lecita, il dissenso dell'avente diritto rileva come elemento costitutivo del fatto tipico poiché la sua assenza esclude l'integrazione della fattispecie oggettiva del reato[93]. Ne consegue tra l'altro che, in tal caso, il dissenso alla permanenza nel sistema non può dunque essere desunto dalla presenza di misure di sicurezza (logiche) la cui rimozione sia indispensabile per accedere ai dati, essendo invece necessario che il titolare dello *ius excludendi* dichiari, in modo espresso o tacito, detto dissenso, oppure lo manifesti attraverso comunicazioni elettroniche (ad es. con un messaggio che avverta che l'accesso ai dati è consentito solo alle persone autorizzate).

Infine, a conclusione dell'analisi circa le condotte del presente reato, bisogna tener presente che la permanenza nel sistema informatico che faccia seguito ad una introduzione illegittima (prima condotta) costituisce un semplice *post-factum* non punibile, né integra la diversa ed autonoma ipotesi del mantenimento (seconda condotta), che presuppone come condotta prodromica l'introduzione legittima; di conseguenza non è possibile ipotizzare il concorso materiale tra l'ipotesi di introduzione abusiva e di mantenimento abusivo.

[93] Come infatti fa notare PECORELLA G., *sub. Art. 615 ter*, in MARINUCCI-DOLCINI, *Codice penale commentato,* IPSOA, Milano, 2011, pag. 5986.

2.1.5 Il requisito dell'abusività

Come si è rilevato *supra,* le condotte penalmente rilevanti sono accompagnate dall'avverbio "abusivamente" e dall'inciso "contro la volontà espressa o tacita di chi ha il diritto di escluderlo".

Il rapporto fra i differenti incisi del reato

Si è ritenuto che entrambi si riferiscano a tutte e due le condotte presenti nella norma e che, quindi, costituiscano una ripetizione dovuta alla volontà di connotare le condotte con il requisito della mancanza di autorizzazione del titolare. Invece, molto semplicemente, basta affermare che nonostante la doppia locuzione, la qualifica di illiceità speciale del legislatore sia unica e consiste nell'assenza del consenso all'accesso, il quale deve sussistere nel momento dell'introduzione e permanere per tutta la durata, comportando altresì l'illiceità della condotta[94].

Altra posizione vuole però attribuire significato autonomo all'avverbio "abusivamente", considerandolo una vera e propria ipotesi di antigiuridicità speciale sganciata dal secondo inciso appena menzionato. Ad essa si oppone tuttavia che, intendendo così il requisito dell'abusività, ci si porrebbe in una posizione incompatibile col bene giuridico tutelato dal momento che si attribuirebbe rilievo a scriminanti non codificate, suscettibili di apprezzamento soggettivo tali da comportare uno svilimento al contenuto del diritto alla privacy[95].

Abusività e Sezioni Unite: il caso dell'utilizzazione abusiva di accesso autorizzato

In realtà, in quest'area, le considerazioni più interessanti si svolgono, specificatamente, nel caso dell'utilizzazione abusiva di un accesso lecitamente autorizzato, argomento che costituisce una delle questioni applicative centrali in questa materia, sulle quali si è imposta, a Sezioni Unite, la Corte di Cassazione.

Con sentenza n. 4694 del 2011 la Corte ha ripercorso, *in primis*, gli orientamenti giurisprudenziali che si sono susseguiti sul caso; per uno di

[94] PICA G., *Diritto penale delle tecnologie informatiche,* UTET, Torino, 1997, pag. 51.
[95] PICA G., *cit.*

questi, il reato dell'articolo 615 ter può anche integrarsi dalla condotta di chi, essendo abilitato all'accesso, si introduca con la password di servizio e raccoglie dati protetti per finalità estranee alle ragioni e agli scopi dell'archivio informatico al quale ha accesso, utilizzando, quindi, il sistema per finalità diverse da quelle a lui consentite. Tale orientamento si fonda sulla considerazione che la norma punisce non solo l'abusiva introduzione ma anche la permanenza abusiva contro la volontà di chi ha il diritto di escluderla che, in questo caso, sarà tacita in quanto, per così dire, costruita in negativo rispetto a quelle attività che, invece, il soggetto agente è legittimato a compiere[96].

L'orientamento estensivo

A supporto di ciò è anche richiamata la sentenza di Cassazione, Sez. V, 8.7.2008, n. 37322, con la quale si ricorda che la violazione dei dispositivi di protezione del sistema informatico non assume rilevanza di per sé, perché non si tratta di un illecito caratterizzato dalla effrazione dei sistemi protettivi, bensì solo come manifestazione di una volontà contraria a quella di chi del sistema legittimamente dispone. L'accesso al sistema è consentito dal titolare per determinate finalità, cosicché se "*il titolo di legittimazione all'accesso viene dall'agente utilizzato per finalità diverse da quelle consentite non vi è dubbio che si configuri il delitto in discussione, dovendosi ritenere che il permanere nel sistema per scopi diversi da quelli previsti avvenga contro la volontà, che*

[96] Nel dettaglio, l'opzione esegetica in oggetto è stata motivata anzitutto sulla base della ravvisata analogia con la fattispecie della violazione di domicilio, considerandosi che entrambi gli illeciti sono caratterizzati dalla manifestazione di una volontà contraria a quella, anche tacita, di chi ha diritto di ammettere ed escludere l'accesso e di consentire la permanenza (nel sistema informatico alla stessa stregua che nel domicilio). Se il titolo di legittimazione all'accesso viene utilizzato dall'agente per finalità diverse da quelle consentite, dovrebbe ritenersi che la permanenza nel sistema informatico avvenga contro la volontà del titolare del diritto di esclusione (C., Sez. V, 7.11.2000 n. 12732; caso Zara). Il caso concerne una vicenda in cui un soggetto, essendo autorizzato solo all'accesso "*per controllare la funzionalità del programma informatico*", si era indebitamente avvalso di tale autorizzazione "*per copiare i dati in quel programma inseriti*", rilevando che "*il delitto di violazione di domicilio è stato notoriamente il modello di questa nuova fattispecie penale, tanto da indurre molti a individuarvi, talora anche criticamente, la tutela di un domicilio informatico"*.

può, per disposizione di legge, anche essere tacita, del titolare del diritto di esclusione"[97].

L'orientamento restrittivo

Rispetto a questo orientamento, la Corte ne evidenzia un altro, totalmente difforme, che, in ogni caso, esclude la configurabilità del reato ex articolo 615 ter per la medesima condotta esposta *supra,* ferma restando la sua responsabilità per gli altri reati eventualmente configurabili.

Quest'interpretazione è sostenuta dalla posizione per cui la sussistenza della volontà contraria dell'avente diritto deve essere verificata esclusivamente con riguardo all'immediato risultato della condotta posta in essere dal soggetto attivo tramite l'accesso al sistema ed il mantenimento al suo interno, non invece a fatti successivi (cioè l'uso illecito dei dati). Come è facile prevedere, questo secondo orientamento si oppone al primo a partire dall'interesse tutelato inteso dalla norma in esame, dal momento che, in questo caso, l'attenzione è concentrata verso il bene giuridico della tutela dei sistemi informatici e telematici piuttosto che, specificatamente, verso quello del domicilio informatico e dell'insito diritto alla privacy[98].

Il caso principiale, richiamato, è quello della sentenza Migliazzo[99] ove si è affermato che "*non integra il reato di accesso abusivo ad un sistema informatico (art. 615 ter) la condotta di coloro che, in qualità rispettivamente di ispettore della Polizia di Stato e di appartenente all'Arma dei Carabinieri, si introducano nel sistema denominato S.D.I*[100]*, considerato che si tratta di soggetti autorizzati all'accesso e, in virtù del medesimo titolo, a prendere*

[97] Per completezza, ecco le altre sentenze a supporto di quest'orientamento: C., Sez. V, 3.2.2009, n. 18006; C., Sez. V, 10.12.2009, n. 2987; C., Sez. V, 16.2.2010, n. 19463; C., Sez. V, 22.9.2010, n. 39620; C., Sez. V, 18.1.2011, n. 24583.

[98] Per altro, a tale motivazione se ne accompagna un'altra, letteraria, tratta dalla formula normativa "abusivamente si introduce". Questa, per la sua ambiguità, potrebbe dare luogo ad imprevedibili e pericolose dilatazioni della fattispecie penale se non fosse intesa nel senso di "accesso non autorizzato", secondo la più corretta espressione di cui alla c.d. "lista minima" della Raccomandazione R(89)9 del Comitato dei Ministri del Consiglio d'Europa, sulla criminalità informatica, approvata il 13.9.1989 ed attuata in Italia con la L. 23.12.1993, n. 547, e, quindi, della locuzione "accesso senza diritto" (*access without right*) impiegata nell'art. 2 della Convenzione del Consiglio d'Europa sulla criminalità informatica (*cyber crime*) fatta a Budapest il 23.11.2001 e ratificata con la L. 18.3.2008, n. 48.

[99] C., Sez. V, 20.12.2007, n. 2534.

[100] Banca dati interforze degli organi di polizia.

cognizione dei dati riservati contenuti nel sistema, anche se i dati acquisiti siano stati trasmessi ad una agenzia investigativa, condotta quest'ultima ipoteticamente sanzionabile per altro e diverso titolo di reato". In sintesi, si era ritenuto, in maniera piuttosto discutibile, che, se per la consumazione del reato "*basti l'intenzione*", da parte del soggetto autorizzato, di fare un successivo uso illecito di quei dati, ne deriverebbe la conseguenza che il reato non sarebbe escluso nemmeno se quell'uso, magari per un ripensamento, non vi fosse più stato[101].

Conclusione simile, per questo secondo orientamento, è stata condivisa nel caso Peperaio[102] nella quale si è detto che la qualificazione di abusività della norma in esame va intesa in senso oggettivo, cioè con riferimento al momento dell'accesso ed alle modalità utilizzate dall'autore per neutralizzare e superare le misure di sicurezza (chiavi fisiche o elettroniche, password, etc.) apprestate dal titolare dello *ius excludendi*. In questo modo, la finalità dell'accesso, se illecita, integrerà eventualmente un diverso titolo di reato e non può, pertanto, condividersi l'interpretazione della norma che individua, per esempio, l'abusività della condotta nel fatto del pubblico ufficiale o dell'incaricato di pubblico servizio che, abilitato ad accedere al sistema informatico, usi tale facoltà per finalità estranee all'ufficio e, quindi, non rispetti le condizioni alle quali era subordinato l'accesso. Una tale lettura della norma, per la Corte, finisce con l'intrecciare le due condotte descritte dall'articolo 615 ter, che sono differenti e alternative, disgiuntamente considerate dal legislatore. Quindi, afferma, "*sarebbe stata pleonastica la descrizione della seconda condotta se*

[101] La stessa interpretazione restrittiva del contenuto della norma è stata poi ulteriormente sviluppata dalla Quinta Sezione con la sentenza n. 26797 del 29 maggio 2008 ove è stato escluso che dovesse rispondere del reato in questione un funzionario di cancelleria il quale, legittimato in forza della sua qualifica ad accedere al sistema informatico dell'amministrazione giudiziaria, lo aveva fatto allo scopo di acquisire notizie riservate che aveva poi indebitamente rivelate a terzi con i quali era in previo accordo; condotta, questa, ritenuta integratrice del solo reato di rivelazione di segreto d'ufficio, previsto dall'art. 326.

[102] C., Sez. VI, 8 ottobre 2008, n. 39290.

la prima fosse integrata anche da chi usa la legittimazione all'accesso per fini diversi da quelli a cui è stato legittimato dal titolare del sistema"[103].

Il principio di diritto delle S.U. n.4694/2011 e le sue motivazioni

Venendo alla posizione conclusiva delle Sezioni Unite, a seguito dei difformi orientamenti, la Corte afferma il principio di diritto per cui "*integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615 ter, la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso al sistema".*

A motivazione di ciò, la Corte ha ritenuto che la questione di diritto controversa non debba essere studiata sotto il profilo delle finalità perseguite da colui che accede o si mantiene nel sistema, poiché la volontà del titolare è connessa soltanto al dato oggettivo della permanenza (per così dire "fisica") dell'agente in esso. Ciò significa che la volontà contraria dell'avente diritto deve essere verificata solo con riferimento al risultato immediato della condotta posta in essere, non già ai fatti successivi. Rilevante sarà, quindi, il profilo oggettivo dell'accesso e del trattenimento nel sistema informatico da parte di un soggetto che sostanzialmente non può ritenersi autorizzato ad accedervi ed a permanervi "*sia allorquando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema sia allorquando ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali l'accesso era a lui consentito*".

In questi casi, ritiene la Corte, è proprio il titolo legittimante l'accesso e la permanenza nel sistema che risulta violato: il soggetto agente opera illegittimamente, in quanto il titolare del sistema medesimo lo ha ammesso

[103] Tra le altre posizioni a supporto di questo secondo orientamento si ricordano: C., Sez. V, 25.6.2009, n. 40078; C., Sez. V, 13.10.2010, n. 38667.

solo a determinate condizioni, in assenza delle quali le operazioni compiute non possono ritenersi coperte dall'autorizzazione ricevuta.

Quindi, il dissenso tacito del titolare non viene desunto dalla finalità che muove la condotta dell'agente, bensì dall'oggettiva violazione delle disposizioni del titolare in ordine all'uso del sistema.

Conseguentemente risulteranno irrilevanti gli eventuali fatti successivi: questi, semmai, saranno frutto di nuovi atti e pertanto, se illeciti, saranno sanzionati con riguardo ad altro titolo di reato (rientrando, ad esempio, nelle previsioni di cui agli artt. 326, 618, 621 e 622 c.p.).

Ne deriva che, nei casi in cui l'agente compia sul sistema un'operazione pienamente consentita dall'autorizzazione ricevuta, ed agisca nei limiti di questa, "*il reato di cui all'art. 615 ter non è configurabile, a prescindere dallo scopo eventualmente perseguito; sicché qualora l'attività autorizzata consista anche nella acquisizione di dati informatici, e l'operatore la esegua nei limiti e nelle forme consentiti dal titolare dello* ius excludendi*, il delitto in esame non può essere individuato anche se degli stessi dati egli si dovesse poi servire per finalità illecite*".

Il giudizio circa l'esistenza del dissenso del *dominus loci* deve assumere come parametro la sussistenza o meno di un'obiettiva violazione, da parte dell'agente, delle prescrizioni impartite dal *dominus* stesso circa l'uso del sistema e non può, quindi, essere formulato unicamente in base alla direzione finalistica della condotta, soggettivamente intesa.

In conclusione, dunque, vengono in rilievo quelle disposizioni che regolano l'accesso al sistema e che stabiliscono per quali attività e per quanto tempo la permanenza si può protrarre, da prendere necessariamente in considerazione, mentre devono ritenersi irrilevanti, ai fini della configurazione della fattispecie, eventuali disposizioni sull'impiego successivo dei dati[104].

[104] Tale conclusione è stata poi condivisa in seguito, come nel caso delle successive sentenze: C., Sez. II, 6.3.2013, n. 13475; C., Sez. V, 8.5.2012, n. 42021.

2.1.6 Altri aspetti rilevanti della fattispecie

Giunti a questo punto dell'analisi dell'articolo 615 ter, rimangono da analizzare alcuni profili conclusivi, peraltro non eccessivamente problematici.

L'elemento soggettivo

A cominciare dall'elemento soggettivo, è richiesto il dolo generico, consistente nella coscienza e volontà di introdursi o mantenersi nell'altrui sistema informatico o telematico, quindi nella memoria interna di un elaboratore, in assenza del consenso del titolare dello *ius excludendi* e con la consapevolezza che questi ha predisposto misure di sicurezza a protezione del sistema. La questione è pacifica anche in giurisprudenza, ove si menziona un solo caso[105] nel quale si è escluso il dolo in riferimento ad un accesso per finalità diverse da quelle per cui era stato autorizzato ma solo per pochi secondi e per prendere visione di soli dati anagrafici di pubblica conoscenza e conoscibilità.

Il momento consumativo del reato

Per quanto concerne la consumazione del reato, ma già lo si è accennato, il reato si consuma, nel caso di introduzione, nel momento in cui sono oltrepassate le barriere a cui è subordinato l'accesso ai dati e ai programmi ivi contenuti; mancherà invece la consumazione quando il soggetto abbia solo iniziato a colloquiare col sistema ma ancora non abbia superato le barriere[106]. Nell'ipotesi di permanenza, invece, il reato si consuma allorquando l'autore si trattiene all'interno del sistema, nel quale si è lecitamente introdotto, nonostante il dissenso del titolare del diritto di esclusione. Si tratterebbe, come è ovvio, di reato permanente la cui consumazione cessa nel momento in cui si interrompe l'accesso, mentre nel primo caso si tratterebbe di un reato a consumazione istantanea.

Il locus commissi delicti

Venendo alla individuazione del luogo di commissione del reato, occorre tenere presente che, di norma, si tratta di accessi virtuali o a distanza

[105] T. Nola 11.12.2007.
[106] MONACO L., *Sub art. 615 ter c.p.,* in *Commentario breve al codice penale,* a cura di CRESPI, STELLA, ZACCALA', 4° Ed., Padova, 2003, pag. 1728.

attraverso un collegamento effettuato con un modem, conseguentemente il reato deve ritenersi perfezionato nel luogo in cui ha fisicamente sede il sistema oggetto di intrusione e non nel luogo in cui si trovi fisicamente l'agente nel momento in cui vengono poste in essere le attività intrusive[107]. Tale posizione è inoltre condivisa da recentissima giurisprudenza[108], per cui il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico non è quello in cui vengono inseriti i dati idonei ad entrare nel sistema bensì quello dove materialmente è collocato il server che elabora e controlla le credenziali di autenticazione del cliente.

Il tentativo

Venendo ora alla configurabilità del tentativo, questo sarà rinvenibile in tutti i casi in cui l'agente, in presenza di una volontà contraria dell'avente diritto, cerchi di aggirare le protezioni, per esempio digitando più password, e non vi riesca. Invece, non si ritiene che sia configurabile il tentativo, nei casi in cui l'agente acceda da lontano o da vicino al sistema, ma non tenti di superare le misure di sicurezza esistenti, in tale ipotesi, infatti, non si è in presenza di atti diretti in modo non equivoco alla violazione delle barriere di protezione e, quindi, della privacy, in quanto il soggetto può ben essersi collegato senza sapere che l'accesso ai dati fosse protetto[109]. Al contrario, secondo un recente orientamento, nel reato di accesso abusivo, trattandosi di un reato di pericolo astratto, non è ammissibile il tentativo perché altrimenti vi sarebbe un'eccessiva anticipazione della soglia di punibilità in violazione del principio di offensività[110].

Le quattro circostanze aggravanti

Proseguendo all'interno dell'articolo 615 ter, ai commi 2° e 3° sono previste quattro circostanze aggravanti caratterizzate da un forte inasprimento della pena edittale.

---

[107] PARODI C., CALICE A., *Responsabilità penali e internet*, IlSole24Ore, Milano, 2001, pag. 67.
[108] C., Sez. I, 27 maggio 2013, n. 40303.
[109] Invece, Nel caso di misure di protezione "fisiche" (come ad es. le porte blindate che precludano l'accesso ai locali in cui è posto il sistema) non è configurabile il tentativo poiché non si tratta di atti diretti in modo non equivoco a violare il sistema informatico ben potendo trattarsi di atti diretti a compiere altri illeciti (ad es. furti, ecc.).
[110] Su tutti ANTOLISEI F., *Manuale di Diritto Penale – Parte speciale I,* Milano, Giuffrè Editore, 2003, pag. 247.

Sono circostanze ad effetto speciale[111], e, le prime, sono caratterizzate dallo specifico ruolo dell'attore del reato per ognuna di queste. La circostanza del comma 2° n.1 prevede un aggravamento della pena per il pubblico ufficiale o incaricato di un pubblico servizio[112] che agisca con abuso dei poteri o con violazione dei doveri inerenti alla sua funzione o servizio, per chi esercita abusivamente la professione di investigatore privato e per chi agisca con abuso della qualità di operatore di sistema. Per quanto concerne quest'ultima posizione soggettiva, in dottrina non vi è univocità di consensi circa il suo intendimento: nell'interpretazione più ampia, si ritiene che rivesta detta qualità chiunque sia legittimato ad operare nel sistema, ivi compreso l'addetto all'immissione dei dati fino a ricomprendere tutti i tecnici dell'informatica, trattandosi di persone che *"operano sul computer"* [113].

Il n.2 tratta, invece, profili di oggettiva gravità della condotta, vale a dire se il colpevole usa violenza su cose o persone per commettere il fatto, oppure è palesemente armato.

Per quanto concerne l'aggravante del n.3, essa riguarda le conseguenze della condotta e, nello specifico, si riferisce alla eventualità che dall'accesso abusivo possa derivare anche il danneggiamento del sistema nel suo complesso o di singole componenti (quali dati, informazioni o programmi in esso contenuti). È bene ricordare, per quanto elementare, che, in questo caso,

---

[111] Per cui secondo la previsione di cui all'art. 63, 3° comma, consentono, a differenza dell'ipotesi base del reato perseguibile a querela, che si proceda d'ufficio.

[112] C'è da dire, tuttavia, che in giurisprudenza l'accesso abusivo ad un sistema informatico (art. 615 ter, 1° co.) e l'accesso commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri o con abuso della qualità di operatore del sistema (art. 615 ter, 2° co., n. 1) sono, invece, considerate due distinte ipotesi di reato, l'applicabilità di una delle quali esclude l'altra secondo il principio di specialità; concernendo il 1° co. l'accesso abusivo ovvero l'intrusione da parte di colui che non sia in alcun modo abilitato, mentre il 2° co. - non costituisce una mera aggravante - ma concerne il caso in cui soggetti abilitati all'accesso abusino di detta abilitazione (C., Sez. V, 30.9. - 16.1.2009, n. 1727).

[113] BORRUSO R., *La tutela del documento e dei dati*, *in Profili penali dell'informatica*, Milano, 1994, pag. 33; tuttavia, per una posizione intermedia sono dotati di tale qualità solo *"quei soggetti che non solo possono legittimamente contattare il sistema, ma che dispongono altresì di una qualificazione professionale ovvero di conoscenze ulteriori e specifiche"* (MUCCIARELLI F., *Commento all'art. 4 della legge 547 del 1993*, in LP, 1996, 102). Per la posizione minoritaria, si ritiene che rivestano la qualità di operatore di sistema le figure soggettive (programmatore, sistemista, analista ecc.) titolari di una maggiore, per qualità e quantità, competenza tecnica, la quale unitamente al ruolo che rivestono all'interno del contesto in cui agiscono le agevola nel momento in cui intendono perpetrare il delitto.

il danneggiamento è conseguenza e non mezzo necessario per addivenire al perfezionamento del reato, altrimenti si dovrebbe applicare l'aggravante prevista al comma 2°, n.2. Assai importante è invece rammentare che, l'aggravante del danneggiamento dev'essere necessariamente una conseguenza non voluta[114], in quanto, altrimenti, dovrà altresì applicarsi la norma sul danneggiamento informatico dell'art. 635 bis, che a breve tratteremo.

Infine, ai sensi del comma 3°, le condotte di cui al 1° ed al 2° comma vengono sanzionate più gravemente[115] qualora abbiano ad oggetto sistemi informatici o telematici di interesse pubblico, tra i quali rientrano i sistemi di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile. Peraltro, a detta di alcuni, tale previsione peccherebbe di indeterminatezza non essendo chiari i criteri in base ai quali il sistema assuma la connotazione pubblicistica facendo scattare l'aggravante in esame[116]. Inoltre, coloro che individuano l'interesse tutelato dalla norma in esame nel domicilio informatico, rilevano l'incongruenza di detta previsione, ritenendone più opportuna la collocazione in altre parti del codice specificamente dedicate alla protezione di interessi pubblici, piuttosto che nell'ambito di una tutela che resterebbe pur sempre di natura privatistica[117].

Il rapporto con altre figure di reato

A conclusione della trattazione dell'articolo 615 ter, permane da analizzare il suo rapporto con le ulteriori figure di reato presenti nel Codice Penale.

Il reato in esame, in quanto, lo si è visto, di pericolo astratto, può concorrere con la falsificazione dei documenti informatici (art. 491 bis), il danneggiamento di sistemi informatici o telematici (art. 635 bis), la frode informatica realizzata attraverso la alterazione dei dati o dei programmi (art. 640 ter) e la rivelazione di documenti segreti di cui si sia venuti a conoscenza

[114] Si veda, in questo senso, MANTOVANI F., *Diritto penale. Parte speciale I. Delitti contro la persona,* Padova, 2011, pag. 547, in tema di reato aggravato dall'evento.
[115] Rispettivamente, con la reclusione da 1 a 5 anni e da 3 a 8 anni.
[116] PARODI C., CALICE A., *Responsabilità penali e internet*, IlSole24Ore, Milano, 2001, pag. 70.
[117] GALDIERI A., *L'introduzione contro la volontà del titolare fa scattare la responsabilità dell'hacker*, in *Giurisprudenza di Merito*, 2001, n.8 , pag. 157.

abusivamente (art. 621). Si ritiene, invece, inammissibile il concorso con la rivelazione del segreto professionale (art. 622) e del segreto industriale (art. 623) in quanto tali delitti presuppongono che l'agente sia detentore legittimo del segreto che indebitamente divulghi.

Tra i più interessanti vi è sicuramente il rapporto con l'art. 640 ter, anche per la forte produzione giurisprudenziale[118] su questo tema, che sarà poi analizzato nel dettaglio nei paragrafi a seguire. Specificamente in tema di *phishing*, vale a dire di quella tecnica volta ad ottenere, tramite artifici e raggiri e inducendo in errore l'utente, le credenziali di autenticazione necessarie ad accedere abusivamente a spazi informatici esclusivi del titolare ed a svolgere, senza autorizzazione, recente giurisprudenza[119] afferma che possono sussistere i reati di cui agli artt. 494 (sostituzione di persona), 615 ter (accesso abusivo a sistemi informatici o telematici), e 640 (truffa).

[118] Si ricorda, da ultimo la sentenza di Cassazione dell'11 marzo 2011, n. 9891, ove in particolare si afferma che integra il reato di frode informatica, e non già soltanto quello di accesso abusivo ad un sistema informatico o telematico, la condotta di introduzione nel sistema informatico delle Poste italiane S.p.A. mediante l'abusiva utilizzazione dei codici di accesso personale di un correntista e di trasferimento fraudolento, in proprio favore, di somme di denaro depositate sul conto corrente del predetto.

[119] T. Milano 7.10.2011.

2.2 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater)

La ratio della norma

La norma prevista dall'articolo 615 quater c.p.[120], anch'essa introdotta tramite la legge n.547/93 di cui *supra,* sanziona l'acquisizione e la diffusione abusiva, con qualsiasi modalità, di mezzi o comunque codici di accesso atti a consentire a chi non è legittimato l'introduzione in un sistema informatico o telematico, protetto da misure di sicurezza. Come è evidente, la finalità di tale fattispecie è quella di prevenire l'uso non autorizzato di quei mezzi che consentono l'accesso al sistema[121]; conseguentemente si vuole reprimere, indipendentemente dal verificarsi dell'evento, tutte quelle condotte prodromiche alla realizzazione del delitto ex. art. 615 ter c.p.. In particolare, l'ipotesi che maggiormente sembra rientrare nella fattispecie in questione, è quella della sostituzione illegittima dell'agente al legittimo titolare del sistema con l'uso della password di quest'ultimo.

Il bene giuridico tutelato

Cominciando, come di consueto, dall'analisi del bene giuridico tutelato, dottrina unanime ritiene che, data la collocazione prossima al prodromico reato di accesso abusivo a sistema informatico o telematico, valgano le stesse considerazioni per tale illecito penale; quindi, si contrappone chi ritiene che l'articolo in esame conferisca una tutela anticipata al domicilio informatico e chi invece ritiene che comporti un rafforzamento della tutela della segretezza dei dati e dei programmi contenuti nell'elaboratore[122]. Tuttavia non manca chi, fornendone una visione più generale, attribuisce alla norma in esame una funzione più ampia di tutela anticipata dei beni giuridici protetti da una

[120] [1] Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.
[2] La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1 e 2 del quarto comma dell'articolo 617 quater.

[121] GALDIERI P., *Teoria e pratica nell'interpretazione del reato informatico*, Giuffrè, Milano, 1997, pag. 158 e anche PECORELLA G., *sub. Art. 615 quater*, in MARINUCCI-DOLCINI, *Codice penale commentato,* IPSOA, Milano, 2011, pag. 5994.

[122] Come nel caso del reato ex. art. 615 ter, le due posizioni sono appoggiate, da un lato, dal GALDIERI, mentre, dall'altro, dal PECORELLA.

serie di norme penali informatiche (e cioè patrimonio, riservatezza, fede pubblica) e la considera, quindi, preordinata a prevenire in via generale la realizzazione di reati informatici, e chi, in termini ancor più ampi, le attribuisce una funzione di tutela anticipata rispetto a tutti gli illeciti che possono essere realizzati una volta superato l'ostacolo rappresentato dalle misure di protezione[123].

La struttura del reato

Sempre sulla falsariga dell'articolo precedentemente analizzato, questo reato è, per larga parte della dottrina, ritenuto di pericolo astratto e, inoltre, vi è chi ritiene che, addirittura, si tratti di una fattispecie di pericolo necessariamente indiretto[124], poiché mira a reprimere condotte idonee a determinare il pericolo di accessi abusivi a loro volta pericolosi per la tutela del bene protetto dall'art. 615 ter. Infatti, sulla stessa linea di pensiero, si pone dottrina la quale ritiene che la sanzione delle condotte di "procurarsi" e di "riprodurre" i mezzi in questione integri un reato di sospetto, perché esse, con qualche difficoltà per il principio di offensività, anticiperebbero la soglia della punibilità ad atti al più preparatori, mentre le restanti condotte costituirebbero ipotesi di reato ostacolo, in quanto volte a prevenire in via generale la realizzazione di reati informatici[125]. Un diverso orientamento ne esclude, invece, la natura di reato di pericolo, in quanto attribuisce alla norma in esame la funzione primaria di prevenire gli accessi abusivi effettuati senza alterare il software e mediante la sostituzione illegittima dell'agente al legittimo titolare con la conseguenza di considerarlo posto a tutela, in via immediata e diretta, della riservatezza dei codici di accesso, che il legislatore considera alla stregua di qualità personali

[123] In questo caso le posizioni sono sostenute rispettivamente da MANTOVANI F., *Diritto Penale – Parte Speciale, delitti contro la persona,* Padova, 2012, pag. 548 e da MAIORANO N., *sub art. 615 quater*, in *Codice Penale Padovani*, pag. 4406.

[124] PECORELLA G., *Il diritto penale dell'informatica*, Cedam, Padova, 2000, pag. 357: Con questo termine si è soliti indicare *"una categoria di reati che, in via del tutto eccezionale, incrimina atti meramente preparatori di altri fatti delittuosi, con riguardo ai quali l'arretramento della soglia di intervento penale ad uno stadio nel quale il pericolo cui il bene esposto è solo indiretto può essere giustificato esclusivamente in presenza di un ragionevole rapporto tra la gravità dell'offesa che si reprime ed il rango del bene protetto, che peraltro nella specie (concernendo la riservatezza dei dati contenuti in un sistema informatico) non si ritiene di rango primario"*.

[125] BERGHELLA R., BLAIOTTA P., *Diritto penale dell'informatica e beni giuridici*, in *Cassazione Penale*, 1995, pag. 1463.

riservate in quanto in grado di identificare la persona, e che poi abilitano a fruire di ogni genere di servizi informatici[126].

L'oggetto materiale del reato: concetto aperto

Proseguendo con l'oggetto materiale del reato, questi saranno codici, parole chiavi e altri mezzi idonei all'accesso, comprendendo, ad esempio, anche informazioni e istruzioni che potrebbero consentire di accedere al sistema informatico o telematico protetto. Solitamente con codice di accesso o parola chiave si intende la chiave che permette un collegamento logico al sistema in questione[127]; in giurisprudenza, si è detto, invece, che i numeri telefonici ed i numeri seriali dei telefoni cellulari possono costituire codici di accesso a sistema punibili dalla norma in esame, dal momento che consentono di individuare l'utenza e l'apparecchio a loro abbinato, e successivamente, se ne viene sfruttata la connessione alla rete di telefonia mobile, che vale come sistema telematico protetto, si andrebbe a integrare il reato in esame[128].

Per quanto concerne il riferimento a qualsiasi mezzo idoneo all'accesso, esso vale come clausola generale di chiusura, ben ricomprendendo, ad esempio, la scheda magnetica da introdurre in un lettore nel quale vi siano registrati dati che permettono l'accesso all'utente. Per una parte della dottrina, fra cui Pecorella, tali mezzi sono riconducibili a tre categorie: i mezzi di accesso fisici[129], i mezzi logici[130] e le indicazioni o istruzioni idonee a realizzare un

---

[126] PICA G, *Diritto penale delle tecnologie informatiche*, UTET, Torino, 1997, pag. 81.

[127] Da non confondere con l'accezione propria del linguaggio informatico che delinea invece una semplice modalità di ricerca: BORRUSO R., *La tutela del documento e dei dati*, in *Profili penali dell'informatica,* Milano, 1994, pag. 30.

[128] In questo senso si vedano C., Sez. II, 17.12.2004; C., Sez. II, 17.1-22.9.2003; C., Sez. II, 21.12.2001. *A contrario*, tuttavia, certa dottrina ha rilevato che dall'abuso di tali strumenti non può derivare alcun pericolo per la riservatezza di dati o programmi, ma solo la lesione di interessi patrimoniali del gestore: PECORELLA G., *Dieci anni di giurisprudenza sui reati informatici: i principali problemi interpretativi sollevati dalle nuove disposizioni*, in *Cocco,Interpretazione e precedente giudiziale in diritto penale*, Padova, 2005, pag. 266.

[129] I quali consentono "direttamente" l'accesso ad un sistema informatico protetto (chiavi meccaniche, chiavi elettroniche e cioè tesserini magnetici di riconoscimento, carte di credito, ecc., di non comune uso per l'alto rischio di contraffazioni, duplicazioni e, più in generale, per la scarsa idoneità a tutelare la sicurezza).

[130] Intesi come parole chiave nel senso di password, ovvero come mezzi che consentono di collegarsi logicamente al sistema.

accesso abusivo[131]. Per altri[132], invece, la norma farebbe, semplicemente, riferimento ad indicazioni o istruzioni idonee a consentire o facilitare l'individuazione, la realizzazione, la riproduzione, la diffusione, la comunicazione o la consegna di mezzi idonei all'accesso a sistemi protetti. Tuttavia, come è ovvio, tale formula di chiusura assurge, necessariamente, a contrastare il costante e rapido progresso tecnico e informatico, così da poter ricondurre all'oggetto materiale ogni strumento di accesso al sistema al momento non ancora esistente, ma riconoscibile in un futuro prossimo[133].

L'analisi delle condotte punite

Giungendo, nel dettaglio, alle condotte sanzionate, esse consistono alternativamente: nell'acquisizione dei mezzi necessari per accedere al sistema informatico altrui, indipendentemente dalla modalità di acquisizione; nel procurare ad altri codici, parole chiavi o altri mezzi idonei a consentire l'accesso abusivo; nel diffondere, comunicare o consegnare a terzi detti mezzi; nel fornire le informazioni, indicazioni, istruzioni idonee a consentire l'accesso ad un sistema informatico altrui protetto da misure di sicurezza. Per quanto concerne invece la detenzione, che è menzionata nella rubrica ma non all'interno della disposizione, secondo alcuni[134] sarebbe da ricomprendersi nella nozione di "procurarsi", mentre per altri[135] non sarebbe penalmente rilevante.

Proprio riguardo al termine di "procurarsi", con esso si intende appropriarsi, in qualsiasi modo[136], dei mezzi necessari per accedere al sistema informatico altrui, il che può avvenire con l'acquisizione materiale della chiave meccanica o della scheda magnetica o anche con l'individuazione dei codici di accesso

[131] Cioè le informazioni tecniche riservate che, pur non consistendo nella comunicazione o consegna del codice di accesso, svelano il metodo idoneo a raggiungere lo scopo ovvero il modo idoneo ad eludere o neutralizzare le misure che proteggono il sistema dagli accessi abusivi.

[132] MUCCIARELLI F., *Commento all'art. 4 della legge 547 del 1993*, in *L'indice penale*, 1996, pag. 105.

[133] Si pensi, ad esempio, quella scienza che tratta degli strumenti biometrici fondati su riconoscimento dal sistema di voce, impronte o reticolo dell'occhio, tutt'ora in corso di perfezionamento ma non ancora del tutto commercializzate.

[134] MANTOVANI F., *Diritto Penale – Parte Speciale, delitti contro la persona,* Padova, 2012, pag. 548.

[135] ATERNO S., *Aspetti problematici dell'art. 615 quater c.p.,* in *Cassazione Penale,* 2000, pag. 389.

[136] *"Anche mediante autonoma elaborazione"*: così espressamente la *Relazione* sul disegno di legge n. 2773 tradottasi poi nella legge 547/93.

attraverso procedimenti logici propri dei computer. La "riproduzione" consiste invece nella realizzazione di una copia abusiva di un codice di accesso pronto all'uso. Con la "diffusione" si intende il divulgare ad un numero indeterminato di persone un certo codice di accesso. Per "comunicazione", permanendo i soliti dubbi interpretativi rispetto al concetto di "diffusione", si ritiene possa da esso differenziarsi in quanto può avere ad oggetto solo mezzi di accesso "logici" ed è rivolta ad una cerchia determinata di persone. La "consegna", infine, riguarda solo cose materiali, come le chiavi di accensione di un computer. Circa invece le indicazioni o istruzioni idonee a realizzare un accesso abusivo, data l'espressione fortemente generica ("fornisce"), si ritiene possa ricomprendere tutte le modalità di condotta in precedenza considerate, cioè la diffusione, la comunicazione e la consegna[137].

Per quanto riguarda l'abusività della condotta, valgono in generale le stesse osservazioni proposte in tema di art. 615 ter c.p. al quale si rinvia. Comunque, secondo prevalente dottrina, l'acquisizione e la diffusione dei codici di accesso e altri mezzi devono realizzarsi in assenza di cause di giustificazione, non mancando, comunque, chi ritiene che il requisito di abusività integri una nota di antigiuridicità speciale[138].

La consumazione del reato

Venendo alla consumazione, essa avverrà nel momento e nel luogo in cui si realizza la condotta tipica e, quindi, allorché il soggetto agente acquisisca la disponibilità del codice entrandone materialmente in possesso o prevenendo autonomamente alla sua individuazione ovvero nel momento in cui viene compiuto il primo atto di diffusione o si realizza la comunicazione o consegna a terzi di tali mezzi eludendo cosi le barriere protettive del sistema. È pacifica, trattandosi di un reato di pericolo astratto, la non configurabilità del tentativo, che comporterebbe un arretramento eccessivo della tutela penale; nonostante ciò, non manca chi, pur ontologicamente, lo ritiene configurabile[139].

---

[137] PECORELLA G., *sub art. 615 quater*, cit., pag. 5996.
[138] Si veda, a riguardo, FONDAROLI C., *La tutela penale dei "beni informatici",* in *Diritto dell'informazione e dell'informatica,* 1996, pag. 514.
[139] MANTOVANI F. cit., pag. 549.

L'elemento soggettivo

Per quanto riguarda l'elemento soggettivo, è richiesto il dolo specifico, ovvero la coscienza e volontà di procurarsi, riprodurre, diffondere, comunicare o consegnare codici di accesso o mezzi simili al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno. La specificità del dolo risulta particolarmente rilevante, poiché impedisce la generica ed automatica applicazione della norma a chiunque comunichi per motivi leciti una password di un sistema a terzi.

Le circostanze aggravanti e rapporti con altre figure di reato

Al comma 2° è previsto un rinvio all'art. 617 quater c.p., comma 4°, nn. 1 e 2 che dà vita ad alcune aggravanti ad effetto speciale[140]. Trattasi delle condotte in danno ad un sistema informatico o telematico utilizzato dallo Stato o da un altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; invece, ex. art. 615 ter c.p., comma 2°, n. 1 e comma 3°, sono richiamate anche le condotte tenute da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso delle qualità di operatore del sistema.

Infine, per quanto riguarda i rapporti con altre figure di reato, dal momento che la norma in esame prevede condotte prodromiche all'art. 615 ter c.p., come detto, esse non possono concorrere nel caso di acquisizione indebita di mezzi idonei ad accedere al sistema informatico, costituendo un antefatto non punibile in caso di realizzazione dell'accesso abusivo[141].

[140] Le quali, ex art. 63 comma 3° c.p., sono così considerate: "Quando per una circostanza la legge stabilisce una pena di specie diversa da quella ordinaria del reato, o si tratta di circostanza ad effetto speciale, l'aumento o la diminuzione per le altre circostanze non opera sulla pena ordinaria del reato, ma sulla pena stabilita per la circostanza anzidetta. Sono circostanze ad effetto speciale quelle che importano un aumento o una diminuzione della pena superiore ad un terzo"-

[141] Se ne ritiene, invece, il concorso, quando siano realizzati dallo stesso agente che in precedenza abbia diffuso a terzi estranei la sua password per consentire loro l'accesso al sistema informatico.

2.3 Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies)

La riforma della legge 48/2008: considerazioni generali

L'articolo in questione[142], come i precedenti, è stato introdotto dalla legge 547/93 ma successivamente modificato dalla legge 48/2008, in quanto la formulazione antecedente era di limitata applicazione giurisprudenziale, poiché assicurava la protezione della funzionalità dei sistemi informatici da una sola e specifica fonte di rischio, vale a dire i cd. virus[143]. Si diceva, tuttavia, che, per rafforzare la tutela del domicilio informatico, venivano sanzionate le condotte che, per la frequenza con la quale si verificano e per i danni che sono in grado di cagionare, costituivano la maggiore minaccia alla sua integrità[144].

Per un diverso orientamento, invece, la fattispecie in esame, in quanto preordinata a proteggere il corretto funzionamento delle tecnologie informatiche ed a salvaguardarle dal danneggiamento, quali appunto i programmi virus, incriminava comportamenti prodromici del danneggiamento di cui all'art. 635 bis c.p.. Dunque, si riteneva che la repressione delle condotte dirette a procurare ad altri la disponibilità di programmi "infetti", ovvero delle condotte prodromiche del danneggiamento del software o dei dati conservati in un sistema, fosse mirata ad evitare *"il danneggiamento del valore del know how racchiuso negli stessi che potrebbero rivelarsi ben più pericolose del danneggiamento fisico dell'hardware in considerazione dell'importanza che il sistema riveste nell'ambito pubblico o privato in cui risulti inserito*"[145]. In quest'ultima ottica, la collocazione della norma in esame tra i delitti contro

[142] [1] Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

[143] Così rileva PECORELLA G., *sub art. 615 quinquies,* in MARINUCCI-DOLCINI, *Codice penale commentato,* IPSOA, Milano, 2011, pag. 6001.

[144] GALDIERI P., *Teoria e pratica dell'interpretazione del reato informatico*, Milano, 1997, pag. 160.

[145] PICA G., *Diritto penale delle tecnologie informatiche,* UTET, 1999, pag. 98.

l'inviolabilità del domicilio appariva incoerente, non trattandosi di comportamenti prodromici alla violazione del domicilio informatico ma piuttosto del danneggiamento, e si riteneva più corretta la collocazione della stessa nell'ambito dei reati contro il patrimonio, immediatamente dopo l'art. 635 bis che, si vedrà, sanziona il danneggiamento informatico.

Per questo motivo, la riforma attuata con la legge 48/2008 estende la protezione contro una più ampia gamma di fonti di rischio come anche ulteriori apparecchiature e dispositivi; vengono inoltre ampliate le condotte sanzionate alle ipotesi di procurarsi, produrre, riprodurre, importare o, comunque, mettere a disposizione di altri detti oggetti; è previsto, infine, che quella che costituiva la caratteristica intrinseca delle fonti di rischio, vale a dire lo scopo o l'effetto di danneggiare interrompere o alterare il funzionamento dei sistemi informatici o telematici oppure i dati o i programmi in esso contenuti o ad esso pertinenti, rappresenti anche il fine perseguito dal soggetto agente con la sua condotta[146].

Si vede, dunque, come le condotte così riformate prescindano dal verificarsi del danneggiamento, costruendo un'anticipazione di tutela secondo lo schema del reato di pericolo astratto "*giustificata, in virtù del principio costituzionale di proporzione, dalla rilevanza del bene giuridico e dalla pericolosità delle condotte tipiche incriminate, le quali implicano, in base all'*id quod plerumque accidit*, la probabilità che il risultato finale dell'azione possa essere il danneggiamento informatico"* [147] . Inoltre, come nel caso dell'articolo precedente, si specifica la collocazione nell'ambito dei reati di pericolo eventualmente indiretto, vale a dire, quei reati che creano il pericolo dell'uso di tali strumenti per danneggiare da parte del detentore ma anche il pericolo della loro diffusione a terzi, i quali, a loro volta, potranno usare per danneggiare tali

[146] Circa la riforma susseguita alla presente legge, si veda PICOTTI L., *Profili di diritto penale sostanziale*, in *La ratifica della Convenzione sul Cybercrime del Consiglio d'Europa*, in *Diritto penale e processo*, 2008, pag. 708.

[147] MONACO L., *Sub art. 615 quinquies c.p.,* in *Commentario breve al codice penale,* a cura di CRESPI, STELLA, ZACCALA', 4° Ed., Padova, 2003, pag. 1731.

strumenti o diffonderli ulteriormente. Invece, per altri ancora, si potrebbe parlare di reato ostacolo, cioè senza offesa[148].

L'oggetto materiale

Passando all'oggetto materiale della condotta, sul quale si è già ampiamente trattato in commento all'art. 615 ter c.p., sono tutelati i sistemi informatici e telematici nonché i dati, le informazioni ed i programmi in esso contenuti. Inoltre, le condotte hanno in oggetto i programmi informatici, i quali devono considerarsi come programmi *"funzionalmente caratterizzati"*[149], vale a dire programmi virus[150], capaci di riprodurre se stessi infettando altri programmi nei quali si insediano con i susseguenti effetti per la sicurezza del sistema[151]. Per certa giurisprudenza[152] non è necessario che si tratti di strumenti idonei a danneggiare, bensì è sufficiente l'idoneità ad interrompere totalmente o parzialmente o ad alterare il funzionamento dei sistemi; l'alterazione si ha quando il programma compia azioni non volute dall'utente, ovvero se ne modifichino i parametri di funzionamento, anche secondo opzioni e possibilità volute dal programma stesso, contro la volontà dell'utilizzatore.

Risulta, tra le altre cose, controverso che nella nozione di programma informatico in questione rientrino anche le istruzioni sul modo di creare un programma infetto: in senso affermativo si ricomprende tale forma di diffusione nella nozione di comunicazione, in senso contrario va evidenziato che le condotte, comunque le si interpretino, hanno ad oggetto specifici strumenti materiali ed immateriali (software), non dunque mere informazioni, pertanto condivisibilmente si rileva l'eccessivo arretramento della tutela penale

[148] Posizioni condivise, rispettivamente, dal DE PONTI e dal MANTOVANI.
[149] PECORELLA G., cit, pag. 6002.
[150] Le forme di contaminazione che tali programmi possono causare sono molteplici: cancellazione totale dell'hard-disk, modifica dei file contenuti in quest'ultimo, alterazione del contenuto del video, perdita di funzionalità specifiche dei programmi o di alcuni di essi fino alla sostituzione o alterazione di funzioni.
[151] Si considerano, tuttavia, come tali da rientrare nel reato in esame i cd. virus benigni che, pur senza avere effetti distruttivi, disturbano il normale funzionamento del sistema, segnalando in vario modo la loro presenza e i programmi worm, che si riproducono incessantemente all'interno della memoria dell' elaboratore in cui vengono inseriti causandone il progressivo esaurimento con il conseguente rallentamento delle normali funzioni del sistema.
[152] A. Bologna 27.3.2008, in CM, 2008, 1066.

che ne deriverebbe[153]. Tra l'altro, è importante evidenziare che di rilievo è anche la distinzione tra l'istruzione automatica di danneggiamento del sistema e l'azione di danneggiamento commessa direttamente dall'agente in quanto solo nel primo caso si è dinanzi ad un programma virus, rilevante per il reato in esame, mentre la seconda ipotesi si connota come azione isolata di disturbo eventualmente rilevante ex art. 635 bis c.p.. Inoltre le condotte sanzionate hanno come oggetto, a seguito della riforma del 2008, anche apparecchiature e dispositivi, dunque viene in considerazione anche l'hardware funzionalmente caratterizzato nel senso della idoneità a danneggiare un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero a favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento[154].

Le condotte del reato

Per quanto concerne invece le condotte del reato, quelle sanzionate sin dal 1993 consistono nel diffondere, comunicare e consegnare programmi e hardware dalle caratteristiche di cui *supra*. La previsione appariva piuttosto ampia ed intesa a ricomprendere esaustivamente ogni forma di distribuzione e circolazione, nonostante ciò, è stata integrata nel nuovo testo con la sanzione onnicomprensiva della condotta di mettere comunque a disposizione di altri i detti oggetti.

Cominciando dalla diffusione, essa implica la messa in circolazione di programmi infetti attuata attraverso le reti telematiche, oppure con la materiale introduzione degli stessi nei sistemi informatici o anche con la vendita di dischi o nastri magnetici che li contengano o, ancora, con l'incorporazione

[153] Alternativamente, tali posizioni sono proposte da D'AIETTI G., *La tutela dei programmi e dei sistemi informatici*, in BORRUSO, BUONUOMO, CORASANITI, D'AIETTI, *Profili penali dell'informatica*, Milano, 1994, pag. 89 e COCCO P., *sub art. 615 quinquies*, in COCCO, AMBROSETTI, *Diritto Penale – Parte Speciale*, Cedam, 2013, pag. 419.

[154] Si pensi, ad esempio, al dongle (chiave di protezione da copie), alla smart card (dispositivo delle dimensioni di una carta di credito che possiede potenzialità di elaborazione e memorizzazione dati ad alta sicurezza), allo skimmer (dispositivo capace di leggere e in certi casi immagazzinare su una memoria i dati della banda magnetica dei badge) o simili, che presentino caratteristiche tali da poter danneggiare i sistemi informatici o telematici.

degli stessi in un adeguato supporto informatico (come un nastro o disco magnetico)[155].

La consegna è, invece, la cessione del supporto fisico sul quale è registrato il programma che viene così posto nella disponibilità altrui. Si tratta di una condotta la cui previsione suscita, secondo alcuni, perplessità, in quanto teoricamente può indicare una attività neutra e, comunque, non sorretta da motivazioni illecite, come nel caso della consegna di un dischetto infetto ad un tecnico perché ne individui e ne rimuova le anomalie, con la conseguenza che di per sé sola non ha un significato univoco e diventa essenziale, ai fini dell'accertamento della sussistenza del reato l'indagine sull'elemento psicologico[156].

Circa la comunicazione, secondo alcuni, essa implica un contatto tra soggetti conferenti e riceventi e si può specificare come comunicazione telematica oppure, più estensivamente, come "*qualsiasi forma di esternazione preordinata alla realizzazione dei programmi in oggetto*"[157]. Secondo altri, invece, essa ha ad oggetto esclusivamente entità immateriali quali i segnali elettronici da cui i dati e i programmi sono rappresentati, cosicché è integrata solo dalla cessione del programma per via telematica, ossia con l'invio del programma attraverso le linee telefoniche cui siano collegati i sistemi informatici, rispettivamente, di chi cede il programma e di chi lo riceve[158]. Per altri ancora, la comunicazione costituisce il mezzo attraverso il quale si realizza la diffusione, cosicché la sua autonoma previsione consente *"di*

[155] Tuttavia, in giurisprudenza, rimane controverso se costituisca un'ipotesi di diffusione rilevante ai sensi della norma in esame l'inserimento del programma nella memoria o nel sistema operativo di un elaboratore collegato in rete con un numero indeterminato di altri sistemi, i quali possano essere a loro volta contagiati per effetto della capacità di trasmigrazione del codice "infetto". Chi nega la rilevanza di tale condotta ritiene che la sola presenza di un programma infetto all'interno di un elaboratore determini, a seconda dei casi, il deterioramento o l'inservibilità del programma o del sistema, con ciò integrando gli estremi del diverso e più grave reato di danneggiamento informatico ex art. 635 bis.

[156] Così PICA G., *Diritto penale delle tecnologie informatiche,* UTET, Torino, 1997, pag. 101.

[157] PARODI C., CALICE A., *Responsabilità penali e internet*, IlSole24Ore, Milano, 2001, pag. 88.

[158] DE PONTI P.*, sub art. 615quinquies*, in MARINUCCI-DOLCINI, *Codice penale commentat*o, IPSOA, Milano, 2011, pag. 6004.

sanzionare altresì il singolo atto iniziale, diretto alla diffusione, prima che il programma nocivo sia effettivamente diffuso fra più sistemi"[159].

La dizione "comunque mettere a disposizione" appare, invece, una clausola di chiusura onnicomprensiva volta a includere nella sfera di rilevanza penale qualsiasi modalità con cui gli oggetti in questione vengano messi nella disponibilità di terzi da parte dell'agente.

Le condotte successive alla riforma del 2008

Come poi si è evidenziato precedentemente, vengono, inoltre, incriminate con la riforma del 2008 le condotte di procurarsi, produrre, riprodurre e importare, chiaramente orientate a colpire il mercato dei programmi o dispositivi illeciti. Se le ultime tre ipotesi non presentano particolari problemi interpretativi, sul procurarsi può discutersi se comprenda anche la mera detenzione; la risposta positiva pare possa evincersi dalla circostanza che la previsione colpisce tutte le condotte da cui può derivare la detenzione, vale a dire la importazione, produzione (in proprio) o riproduzione e il procurarsi (o acquisire consapevolmente) i detti oggetti. Infine, a segnare con chiarezza i contorni dell'illecito anche sul piano oggettivo, vi è lo scopo specifico che deve caratterizzare le condotte in questione, oltre alla natura degli oggetti acquisiti o prodotti. Per questo motivo, assai significativo sarà, almeno sul piano probatorio, il numero degli oggetti detenuti (prodotti o acquisiti)[160].

L'elemento soggettivo

Trattando l'elemento soggettivo, prima della riforma del 2008 si riteneva sufficiente il dolo generico, vale a dire la coscienza e volontà di diffondere, comunicare o consegnare un programma informatico con la consapevolezza che esso, inserito in un sistema informatico, ne comporta il danneggiamento delle componenti fisiche o logiche, ovvero l'interruzione o l'alterazione del funzionamento. Quindi, il dolo in questione richiedeva la consapevolezza

[159] PICA G., *cit,* pag. 101.

[160] La Convenzione di Budapest, infatti, all' art. 6 1.b, consentiva alle parti di incriminare le condotte in questione solo se aventi ad oggetto un certo numero di programmi o dispositivi illeciti. Si veda su ciò, in dettaglio, AMATO G., *Contrasto specifico all'uso di dispositivi*, in *Guida al diritto,* 2008, pag. 58.

dell'esistenza e della natura del programma virus messo in circolazione nonché la volontà di diffonderlo[161].

Il nuovo testo richiede, invece, il dolo specifico "*di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento"*[162], il che restringe sul piano soggettivo l'ampiezza della incriminazione; è quindi richiesto che la condotta sia univocamente indirizzata a tal fine, ma ovviamente il dato si riverbera, come abbiano già evidenziato, sulle caratteristiche di software e hardware, oggetto materiale delle condotte in questione, altrimenti rimanendo l'inammissibile discrimine tra condotte lecite e illecite basato esclusivamente sul dato soggettivo[163].

Consumazione e tentativo

Proseguendo con l'analisi della fattispecie, essa si consuma già con la mera detenzione consapevole degli oggetti in questione, derivanti da riproduzione, produzione, acquisizione o importazione. Nel caso della consegna, invece, il reato si consuma con la *traditio* del supporto che contiene il virus. Non è, come ovvio, necessario che il programma o dispositivo produca i suoi effetti nocivi perchè il reato si consideri consumato.

Infine, quanto al tentativo, sembra doversi escludere sia per evitare l'eccessivo arretramento della soglia di rilevanza penale, non consentito dal principio di offensività sia perché, altrimenti, si finirebbe per sanzionare la mera ideazione degli oggetti pericolosi contro ogni principio penalistico.

---

[161] Infatti a riprova di ciò, in T. Bologna, Sez. I, 22.12.2005, n. 1823, non si esigeva che il fine dell'azione fosse la distruzione o il danneggiamento del sistema informatico. Tuttavia, in dottrina, si era detto che la previsione poteva ingenerare la preoccupazione della sanzione di attività professionali volte alla verifica della sicurezza informatica e alle stesse attività di studio e ricerca nell'ambito della sicurezza informatica (per quanto potesse affermarsi la presenza di cause di giustificazione), perplessità che non sarebbero state superate nemmeno dalla previsione di un dolo specifico di mero danno o vantaggio.

[162] MANTOVANI F., *Diritto Penale – Parte Speciale, delitti contro la persona,* Padova, 2012, pag. 552.

[163] rileva così PICOTTI L., *Profili di diritto penale sostanziale*, in *La ratifica della Convenzione sul Cybercrime del Consiglio d'Europa*, in *Diritto penale e processo*, 2008, pag. 710.

2.4 Violazione della corrispondenza e delle comunicazioni telefoniche, informatiche e telematiche (art. 616, 617 - 617 sexies)

Per quanto riguarda gli articoli trattati nel presente paragrafo, dal momento che il bene giuridico della riservatezza non si pone sempre in primo piano, come per i reati sin ora affrontati, essi saranno sinteticamente analizzati, ponendo alla luce gli aspetti che più rilevano in tema di privacy.

L'art. 616, la condotta di rivelazione

Cominciando con l'art. 616 c.p.[164], rubricato "Violazione, sottrazione e soppressione della corrispondenza", il bene giuridico tutelato è quello della libertà e segretezza della corrispondenza[165]. Tuttavia, tale reato sanziona distinte modalità di aggressione alla libertà e alla segretezza della corrispondenza, ciascuna delle quali danneggia o pone in pericolo ulteriori singoli beni giuridici che, però, sono ontologicamente autonomi per quanto riconducibili ai citati principi costituzionali[166], fra i quali la riservatezza.

Sul concetto di segreto, possiamo prendere per buona la nota posizione del Crespi che lo definisce come *"una relazione che intercorre tra la conoscenza di cose o fatti ed un determinato soggetto"*[167], caratterizzata dal versante attivo, da una posizione di potere di conferire la qualità di segretezza ad una notizia, e sul versante passivo, da un dovere dei terzi di astenersi dal condividere le informazioni precluse.

---

[164] [1] Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da euro 30 a euro 516.
[2] Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni.
[3] Il delitto è punibile a querela della persona offesa.
[4] Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza.

[165] Beni giuridici che sono considerati inviolabili ai sensi dell'art. 15 Cost come estrinsecazione della libertà personale e di manifestazione del pensiero ex artt. 13 e 21 Cost.

[166] Per le posizioni dottrinali in materia, si veda, su tutti, ANTOLISEI F., *Manuale di Diritto Penale – Parte speciale I,* Milano, Giuffrè Editore, 2008, pag. 250.

[167] CRESPI A., *La tutela penale del segreto*, Palermo, 1952, pag. 7.

L'ipotesi che qui interessa è, tuttavia, quella della temporanea sottrazione o distrazione di corrispondenza aperta al fine di prenderne o farne prendere a terzi conoscenza, la quale richiede una ancor più articolata ricostruzione del bene giuridico. La norma, da un lato, completa e rafforza la descritta tutela anticipata del segreto privato, potendo ben riguardare corrispondenza originariamente chiusa e rinvenuta per le più diverse ragioni aperta e, dall'altro, nell'ipotesi di corrispondenza *ab origine* priva del vincolo di segretezza (come nel caso di una cartolina illustrata), offre tutela anticipata al bene giuridico della riservatezza, la cui offesa è sanzionata dalla fattispecie di rivelazione prevista dall'art. 616 c.p., comma 2°.

Infatti, la natura del bene giuridico offeso dalla condotta delineata nell'art. 616, comma 2°, che sanziona, per l'appunto, la rivelazione del contenuto della corrispondenza, chiusa o aperta, da parte di chi ne abbia già preso cognizione, direttamente oppure in esito alla sottrazione o distrazione a ciò finalizzata, non è la segretezza; la fattispecie in questione appresta, in realtà, tutela alla riservatezza del contenuto della privata corrispondenza, cioè al non volere veder reso pubblico, o comunque diffuso indiscriminatamente, anche ad un vasto numero di persone, il contenuto di una corrispondenza destinata ad un ambito di diffusione familiare o in ogni caso estremamente limitato[168].

Detto ciò, è importante ricordare che l'oggetto del reato, ovvero la corrispondenza chiusa o aperta, può essere, ex. comma 4°, epistolare, telegrafica, telefonica, telematica, informatica oppure ogni altra forma di comunicazione a distanza[169].

Vedendo nel dettaglio la condotta del comma 2°, cioè la rivelazione, senza giusta causa, del contenuto della corrispondenza, illecitamente conosciuta,

[168] Eppure, lo si è visto nei capitoli precedenti, parte della dottrina si contrappone alla tesi della reciproca autonomia tra i concetti di segretezza e riservatezza, con l'effetto di ricondurre l'oggetto giuridico dell'intero articolo in commento, salvo le ipotesi di soppressione e distruzione, ad un'assorbente categoria generale di "riservatezza", rispetto alla quale il concetto di segretezza viene ricostruito come mera ipotesi speciale: PATRONO P., voce *Privacy e vita privata (dir. pen.)*, in *Enciclopedia del diritto,* Vol. XXXV, Milano, 1986, pag. 565.

[169] Essa opera come concetto di chiusura onnicomprensivo, in linea con le posizioni dettate dalla Carta Europea dei Diritti dell'Uomo, secondo l'art. 8.

solo se dal fatto deriva nocumento, va rilevato che la norma presuppone la presa di cognizione sanzionata dal comma 1°, sviluppandosi come reato complesso in senso lato[170]. Inoltre, come si è accennato prima, dal momento che tale condotta ha come oggetto di tutela non solo la segretezza del contenuto della corrispondenza, ma anche la riservatezza, si ritiene integrato il reato avente come oggetto non solo una corrispondenza chiusa, ma anche inviata aperta, e perciò non segreta, ad un ambito di diffusione circoscritto. Tra l'altro, questa ipotesi di rivelazione è sanzionata più gravemente rispetto alle fattispecie contemplate dal 1° comma, per cui ci si è chiesto se possa assurgere a reato autonomo, o se, al contrario, essa sia qualificabile come circostanza. Probabilmente la posizione maggiormente condivisa è quella che la riconosce quale ipotesi di reato autonomo: l'enunciazione dell'art. 616, 2° comma. non si esaurisce infatti, come sostenuto dai fautori della tesi circostanziale, in un mero "quid pluris*, che viene ad aggiungersi al fatto costituente una delle ipotesi tipiche del reato"* di cui al 1° comma, ma descrive in realtà, del tutto autonomamente rispetto a tali condotte, *"un nuovo modo di atteggiarsi della condotta del colpevole"*[171].

Circa il concetto di nocumento, esso comprende qualsiasi pregiudizio giuridicamente rilevante ad interessi pubblici o privati, di natura patrimoniale o anche solo morale, patito in conseguenza della rivelazione dal mittente, dal destinatario o anche da terzi soggetti[172].

Invece, sul concetto di giusta causa, è spesso richiamato il criterio del bilanciamento d'interessi in conflitto, secondo il quale dovrebbe ritenersi la presenza di una giusta causa qualora l'interesse perseguito dal soggetto agente

[170] Col quale si intende il reato in cui la realizzazione dell'intera sequenza criminosa comporta la punibilità unicamente a titolo, in questo caso, di rivelazione.
[171] Su tutti le due posizioni sono condivise, rispettivamente, dal MANZINI e da ANTOLISEI.
[172] Permane, tuttavia, un dibattito circa la sua natura di elemento costitutivo quale evento del reato (ANTOLISEI), e condizione obbiettiva di punibilità (MANZINI), con le ovvie conseguenze in tema di elemento soggettivo del reato.

attraverso la rivelazione sia di rilevanza superiore, o quantomeno pari, a quello leso attraverso tale condotta[173].

Venendo all'elemento soggettivo del capoverso da noi analizzato, cioè la rivelazione, è richiesto il dolo generico[174] ovvero la coscienza e volontà del soggetto agente di rivelare, senza giusta causa, il contenuto di corrispondenza chiusa o aperta, a lui non diretta. Infine, tale fattispecie si consuma, qualora si qualifichi il nocumento come condizione obiettiva di punibilità, con l'effettiva percezione della notizia da parte del destinatario, o dei destinatari, della rivelazione, essendo altrimenti integrato il tentativo. La consumazione coinciderà, invece, con la realizzazione del nocumento, con conseguente ampliamento dell'area del tentativo fino alla effettiva percezione della notizia, se si qualifichi il nocumento come di elemento essenziale del reato.

L'art. 617

Giungendo ora all'analisi dell'art. 617 c.p.[175], rubricato "Cognizione, interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche", anch'esso, per la dottrina prevalente, è posto a tutela della libertà e segretezza delle comunicazioni e conversazioni telefoniche e telegrafiche. C'è da dire, però, che ben analizzando la condotta di presa di cognizione, è offeso il diritto alla segretezza nonché il diritto di ciascuno alla non conoscenza da parte di terzi di notizie relative alla propria vita privata, rientrando, a pieno titolo, nel diritto alla riservatezza. Anche per la condotta di rivelazione, a ben vedere, il bene giuridico in questione sarà la riservatezza dei soggetti, cioè il diritto a non veder pubblicato, ossia diffuso indiscriminatamente o comunque ad un vasto numero di persone, il contenuto

[173] Così CRISPI A, *cit.,* pag. 93.

[174] Che muterà, invece, in specifico, qualora si accetti la posizione che accolga il nocumento come evento del reato.

[175] [1] Chiunque, fraudolentemente, prende cognizione di una comunicazione o di una conversazione, telefoniche o telegrafiche, tra altre persone o comunque a lui non dirette, ovvero le interrompe o le impedisce è punito con la reclusione da sei mesi a quattro anni.
[2] Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni o delle conversazioni indicate nella prima parte di questo articolo.

delle conversazioni o comunicazioni intercorse, di cui un terzo sia, anche occasionalmente, venuto a conoscenza.

Analizzando l' oggetto materiale del reato, queste saranno le comunicazioni[176] e conversazioni[177] telefoniche o telegrafiche, intercorrenti tra persone diverse dal soggetto agente. Essendo rilevante, come detto, il secondo capoverso per quanto concerne il diritto alla riservatezza, tale condotta prevede un reato autonomo che sanziona chiunque, in possesso del contenuto di comunicazioni telefoniche o telegrafiche, lo riveli, in tutto o in parte, attraverso mezzi di informazione al pubblico. La fattispecie in esame non presuppone che le conversazioni o comunicazioni, il cui contenuto viene rivelato, debbano essere state oggetto della fraudolenta captazione prevista dall'art. 617, comma 1°, in quanto è sufficiente che il soggetto agente abbia in qualsiasi modo acquisito la conoscenza del contenuto di una comunicazione in atto. La *ratio* di questa fattispecie è di evitare che il soggetto che abbia captato, per qualsiasi via, anche lecita, una conversazione privata intercorrente fra terzi soggetti, possa impunemente renderne pubblico il contenuto[178].

Circa l'elemento soggettivo, è richiesto semplicemente il dolo generico, che dovrà ricoprire tanto le condotte tipiche quanto il carattere fraudolento delle stesse.

L'art. 617 bis

Venendo ora al contenuto dell'art. 617 bis c.p.[179], tale fattispecie si configura come reato di pericolo che fornisce una tutela anticipata ai medesimi beni giuridici sin ora menzionati, ovvero la segretezza e la libertà di conversazioni

[176] Riprendendo la posizione del MANTOVANI, si intende "*comunicazione, la trasmissione, con qualsiasi mezzo, del pensiero umano tra due o più soggetti*".

[177] Ritenuta semplicemente una *species* di comunicazione.

[178] Si contrappone a tale impostazione quella dottrina che restringe la portata della norma alle sole ipotesi di rivelazione del contenuto di comunicazioni fraudolentemente intercettate, ritenendo "assurda" l'ipotesi di rendere penalmente perseguibile la diffusione di notizie lecitamente, o anche solo non fraudolentemente, acquisite: VIGNA-DUBOLINO, *Segreto*, in ED, XLI, Milano, 1989, pag. 1079.

[179] "Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche": [1] Chiunque, fuori dei casi consentiti dalla legge, installa apparati, strumenti, parti di apparati o di strumenti al fine di intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone è punito con la reclusione da uno a quattro anni.

e comunicazioni telefoniche o telegrafiche, conseguentemente, come per l'articolo precedente, non può negarsi lo stretto contatto fra tali beni giuridici e l'interesse della riservatezza, ontologicamente connaturati. Possiamo affermare, quindi, che l'articolo in questione tuteli anche, seppur indirettamente, la privacy di quei soggetti le cui conversazioni private possono essere oggetto di intercettazione. Sono oggetto di incriminazione le condotte più gravi e pericolose prodromiche alla realizzazione dei fatti di intercettazione o interruzione dell'articolo precedente, al fine di porre un freno alla facile possibilità di reperire sul mercato tutte quelle apparecchiature idonee alle intercettazioni abusive, punendo, in un certo senso, fatti che sembrano costituire niente più che il tentativo delle condotte dell'art. 617[180][181].
La condotta consiste nell'installazione di apparati o strumenti idonei ad intercettare o impedire le conversazioni o comunicazioni telegrafiche o telefoniche fra persone diverse dal soggetto agente. È previsto, inoltre, il dolo specifico, in quanto il delitto dev'essere commesso al fine di intercettare o impedire comunicazioni telefoniche o telegrafiche intercorrenti fra terzi.

L'art. 617 ter

Circa invece l'art. 617 ter c.p., in cui è punito chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma falsamente, in tutto o in parte, il testo di una comunicazione o di una conversazione telegrafica o telefonica ovvero altera o sopprime in tutto o in parte il contenuto di una comunicazione o di una conversazione telegrafica o telefonica vera, anche solo occasionalmente intercettata, vi è da dire che, sebbene permangano come sfondo i beni giuridici menzionati sin'ora, è difficilmente configurabile anche la presenza del bene giuridico della riservatezza, quantomeno ad un livello tale che si possa parlare di tutela penale nei suoi confronti. Infatti, ci si sposta più sulla genuinità e veridicità delle comunicazioni, rientrando nella categoria dei reati di falso, piuttosto che sulla privacy dei soggetti passivi

[180] In questo senso molto chiaro è ANTOLISEI F., *Manuale di Diritto Penale – Parte speciale I,* Milano, Giuffrè Editore, 2008, pag. 260.
[181] Aspetto per altro ribadito dalla seguente sentenza di Cassazione: Cass. Pen. Sez. V, 10/11/2004, n. 48285.

coinvolti. Certamente, tuttavia, non può dirsi che la riservatezza sia totalmente esclusa, quantomeno nell'alveo dei diritti che, anche solo trasversalmente, si incontrano con questa fattispecie e, infatti, ben potrebbe rientrare in gioco quantomeno di fronte ad un concorso fra il reato ora citato ed il già analizzato art. 617 c.p..

L'art. 617 quater

Per quanto invece riguarda l'art. 617 quater c.p.[182], rubricato "Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche", sono qui tutelate la segretezza, la libertà e la riservatezza delle comunicazioni relative ad un sistema informatico o telematico intercorrenti tra più sistemi, estendendo l'apparato sanzionatorio dell'art. 617 c.p., del quale ripercorre la struttura. Infatti, la fraudolenta intercettazione del contenuto delle comunicazioni informatiche o telematiche viola la segretezza del contenuto di tali comunicazioni, di cui è punita le mera apprensione, mentre ne offendono la libertà e la regolarità le condotte di interruzione e impedimento. Invece, la condotta di rivelazione tipizzata dall'autonoma fattispecie di cui al comma 2°, tutela il differente bene giuridico della riservatezza delle comunicazioni. Viene sanzionata, infatti, non già la fraudolenta intercettazione, bensì la indiscriminata divulgazione al pubblico del contenuto di una comunicazione, anche se non fraudolentemente captata[183].

L'oggetto materiale del reato è ogni comunicazione relativa ad un sistema informatico o telematico, sul significato dei quali ci si è già soffermati *supra.*

La condotta di nostro interesse è, ovviamente, quella della rivelazione, così come nel caso dello speculare art. 617 c.p. al quale si rinvia circa il significato

---

[182] [1] Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.
[2] Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

[183] Si ricorda, come nel caso dell'art. 617, che altra dottrina supera tali distinzioni, ritenendo sufficiente ricondurre l'oggetto di tutela della norma ad un generale e sfumato concetto di riservatezza delle comunicazioni, quale "formula riassuntiva" dei beni sopra specificati: ROSSI-VANNINI, *La criminalità informatica: le tipologie di computer crimes di cui alla l. 547/93 dirette alla tutela della riservatezza e del segreto*, in *Rivista trimestrale di diritto penale dell'economia*, 1994, pag. 437.

del concetto; tuttavia, in questo caso, non è richiesta la fraudolenza della condotta di rivelazione. Tra l'altro, come per l'art. 617 c.p., si ripropone la *vexata quaestio* di dover ritenere necessaria anche la preesistenza della condotta del comma 1° affinché possa configurarsi quella del comma successivo, oppure quest'ultima gode di piena autonomia. Per gran parte della dottrina[184], tale prodromicità non deve, per l'appunto, tradursi nella necessità di richiedere anche la condotta antecedente per il perfezionamento della rivelazione. Con tale articolo, l'art. 617 quater c.p. condivide anche la necessarietà del dolo generico.

L'art. 617 quinquies

L'art. 617 quinquies c.p.[185] ripercorre, invece, l'ossatura dell'art. 617 bis, sviluppandosi come reato di pericolo, offrendo tutela anticipata al bene giuridico della segretezza e libertà delle comunicazioni informatiche o telematiche, la cui offesa, si è visto, è sanzionata dall'art. 617 quater c.p.. Sono incriminate le più gravi condotte prodromiche alla realizzazione dei fatti di intercettazione, impedimento o interruzione di cui al precedente articolo. A seguito dell'applicazione giurisprudenziale, lo si è individuato come reato di pericolo concreto poiché è richiesto l'accertamento giudiziale dell'effettiva potenzialità lesiva del materiale installato[186].

Tuttavia, c'è da dire che autorevole dottrina[187] ha criticato l'esistenza del reato in esame, poiché considerato "*inutile doppione*" dell'art. 617 bis c.p. che, in combinato disposto con l'art. 623 bis c.p.[188], sarebbe già in grado di ricomprendere le fattispecie incriminate dall' art. 617 quinquies c.p.. Per

[184] Fra cui, ANTOLISEI, CORASANITI e AMATO, *sub art. 617 quater*, in *Cod. pen.* Padovani, pag. 3813.

[185] "Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche": [1] Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.
[2] La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617 quater.

[186] In questo senso, PECORELLA G., *Il diritto penale dell'informatica*, Padova, 2006, pag. 305.

[187] MANTOVANI F., *Diritto Penale – Parte Speciale, delitti contro la persona,* Padova, 2012, pag. 591.

[188] Il quale, semplicemente, dispone che " Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni, immagini od altri dati."

quanto riguarda il rapporto di tale reato con il bene giuridico della riservatezza, si deve dunque rinviare alle considerazioni condivise in tema di art. 617 bis c.p., così come anche per le condotte, avendosi come differenza solamente l'oggetto materiale del reato. Tuttavia, bisogna rammentare che, mentre l'art. 617 bis prevede solamente a titolo di dolo specifico che l'installazione sia effettuata dal soggetto agente al fine di intercettare o impedire comunicazioni telefoniche o telegrafiche, la norma in commento richiede invece espressamente, a titolo di elemento materiale del reato, che le apparecchiature installate siano "atte", cioè concretamente idonee, alla intercettazione; per questo motivo è richiesto, al contrario dell'art. 617 bis, il dolo generico[189].

L'art. 617 sexies

Infine, l'art. 617 sexies c.p.[190], rubricato "Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche", riproduce, in materia di comunicazioni informatiche e telematiche, la disciplina che l'art. 617 ter c.p. riserva alle comunicazioni telefoniche o telegrafiche. Conseguentemente, come per tale reato, il riferimento al bene giuridico alla riservatezza è configurabile esclusivamente alla lontana, in quanto, nemmeno indirettamente può dirsi tutelato dalla norma in esame a meno che non si accolga la posizione dottrinaria che ingloba la libertà e la segretezza delle comunicazioni in un ampio concetto di riservatezza.

[189] Permane tuttavia certa dottrina che, comunque, ritiene che tale reato mantenga il dolo specifico dello speculare art. 617 bis: GARGIULO R.,*sub art. 617 quinquies*, in *Comm. LATTANZI-LUPO*, XI, 2, pag. 1517.

[190] [1] Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.

2.5 Danneggiamento di informazioni, dati e programmi e sistemi informatici(635 bis, 635 ter, 635 quater, 635 quinquies)

Gli articoli seguenti sono stati introdotti, eccetto il primo, che nasce con la legge 547/93, con la successiva legge 48/2008 [191] , dando vita ad un microsistema penale in tema di danneggiamento informatico. Dal momento che questi articoli sono inseriti nel titolo dei reati contro il patrimonio, conseguentemente gli interessi tutelati da dette norme comprenderanno anche il bene giuridico del patrimonio, sviluppando reati plurioffensivi nel momento in cui vengono ricompresi ulteriori interessi.

L'art. 635 bis: l'oggetto giuridico

L'art. 635 bis c.p.[192], anch'esso in seguito riformato dalla legge del 2008 è rubricato "Danneggiamento di informazioni, dati o programmi informatici" e, nel corso della sua riformulazione, è stato scorporato di parte della sua normativa, in quanto, parte di esso, è stato previsto, e più pesantemente sanzionato, nel nuovo 635 quater c.p..

L'introduzione di quest'articolo non costituisce, tuttavia, l'unica ipotesi di danneggiamento di tali sistemi in quanto, lo si è visto, una tutela simile è apprestata dagli artt. 615 quinquies c.p. e 617 quater c.p., i quali, però, sono posti a tutela della persona e non, invece, del patrimonio.

L'oggetto giuridico della tutela penale apprestata dalla norma, oltre che, come è ovvio, il patrimonio altrui, tenuto conto che l'ordinamento prevede ulteriori fattispecie riguardanti la tutela delle strutture informatiche e telematiche, deve ritenersi limitato all' *"inviolabilità del possesso e della disponibilità (in fatto) delle cose-oggetto materiale della condotta"*, cioè "*l'integrità fisica delle apparecchiature e delle istruzioni di funzionamento incise su taluni loro*

[191] Ratificante la Convenzione del Consiglio d'Europa sulla criminalità informatica (*Cybercrime)* fatta a Budapest il 23 novembre 2001. L'art. 5 della legge di ratifica è intervenuto ad implementare lo strumentario sanzionatorio diretto a punire le condotte che si risolvono in un attentato all'integrità dei dati o dei sistemi informatici.

[192] [1] Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
[2] Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

componenti" [193] . Eppure, una posizione di questo tipo deve ritenersi incompleta; non può infatti negarsi che, di fronte ad una condotta come quelle previste nella fattispecie, anche il bene giuridico della riservatezza debba ritenersi, almeno trasversalmente coinvolto tutte le volte in cui una ingente mole di dati venga illecitamente manomessa. Sul tema, inoltre, si è pronunciata anche la giurisprudenza circa la necessità di un reato di questo tipo, che si differenziasse dal danneggiamento generale; i giudici di legittimità infatti, circa l'insussistenza del "vuoto di tutela" che avrebbe dovuto giustificare la creazione della nuova figura criminosa, ha affermato che, antecedentemente all'entrata in vigore della legge 547/93, che ha introdotto in materia la speciale ipotesi criminosa in esame, la condotta consistente nella cancellazione di dati dalla memoria di un computer in modo tale da renderne necessaria la creazione di nuovi integrava un'ipotesi di danneggiamento ai sensi dell'art. 635 in quanto, mediante la distruzione di un bene immateriale, produceva l'effetto di rendere inservibile l'elaboratore; di conseguenza tra il delitto di cui all'art. 635 e l'analoga speciale fattispecie criminosa prevista dall'art. 635 bis esiste un rapporto di successione di leggi nel tempo, regolato dall'art. 2[194].

…Segue: le condotte

Venendo al trattamento delle condotte, esse sono, per buona parte, le medesime rinvenibili nell'art. 635 di danneggiamento. Esso rientra nella categoria dei reati "a forma libera" [195] : per distruzione si deve intendere l'eliminazione, nella cosa, della sua funzione strumentale di soddisfacimento di bisogni umani, materiali o spirituali, che la stessa aveva prima della condotta criminosa; il deterioramento consiste nella diminuzione della funzione strumentale della cosa, della sua utilizzabilità. Per quanto concerne la "cancellazione", l'"alterazione" e la "soppressione", esse sono state esplicitamente menzionate dall'art. 4 sia della Convenzione Cybercrime che

[193] In questo senso MARINI.
[194] Così in Cass. Pen. Sez. Unite, 09/10/1996, n. 1282.
[195] Con i quali si intendono quei i reati in cui la fattispecie è descritta facendo riferimento all'evento, potendo essere le più varie le modalità della azione.

della Decisione quadro 24.2.2005, n. 2005/222/GAI, in quanto specificamente riferibili al peculiare oggetto passivo costituito da "informazioni, dati o programmi informatici". Per cancellazione deve intendersi la rimozione totale o parziale dell'oggetto materiale del reato[196]; alterazione significa la modifica, in tutto in parte, di dati informazioni o programmi.

Non si vede, però, perché non sia stata altresì aggiunta alla locuzione "deteriora", quella più ampia e forse più adeguata di "danneggia", che del resto è poi stata utilizzata dallo stesso legislatore nel successivo art. 635 quater. In realtà anche i "dati" ed a maggior ragione le "informazioni" ed i "programmi" sono suscettibili di esser "resi inservibili" e dunque giuridicamente "danneggiati", con interventi di alterazione o manipolazione riguardanti il solo software, che non intaccano l'integrità dei supporti o dell'hardware.

Per quanto riguarda l'oggetto materiale della condotta, del quale significato si è evidenziato *supra,*è richiesto che esso sia "altrui"[197].

Inoltre, c'è da dire che l'elemento caratteristico del danneggiamento riguardante il settore informatico è appunto quella del suo potere di incidere esclusivamente sul software (ferme restando l'integrità fisica della parte hardware) o sui dati o sulle notizie in esso contenute, per questo motivo si è rilevato che i limiti in cui l'introduzione nel codice dell'art. 635 bis era necessaria appaiono chiari: ferma l'applicabilità della disposizione generale sul danneggiamento per ciò che riguardava la tutela dell'inviolabilità della parte

[196] La giurisprudenza ha inoltre disposto che è integrato il delitto la cancellazione di dati informatici, ancorché questi possano essere recuperati attraverso una complessa procedura tecnica che richiede l'uso di particolari sistemi applicativi e presuppone specifiche conoscenze (C., Sez. V, 18.11.2011-5.3.2012, n. 8555, in un caso in cui un dipendente aveva cancellato, dal computer affidatogli dal datore di lavoro per motivi lavorativi, un numero rilevante di dati, i cui files erano stati recuperati grazie all'intervento di un tecnico informatico specializzato).

[197] Tale requisito fa sorgere il problema se il proprietario della cosa possa essere soggetto attivo del reato, indicato come commissibile da "chiunque" e, quindi, da ritenersi tendenzialmente reato "comune"; la dottrina, dopo aver rilevato come, in campo penale, il requisito dell'"altruità" sia definibile solo in funzione e in stretta correlazione con l'oggetto giuridico del reato, nei delitti contro il patrimonio volta a volta ha ritenuto che la cosa è "altrui": 1) quando è in proprietà di altri, con conseguente esclusione della soggettività attiva per il proprietario; 2) quando sulla stessa altri hanno un diritto di godimento o il possesso o la semplice detenzione, o una mera relazione di fatto, persino di origine illecita. Conseguentemente l'«altruità svolge una funzione negativa stando a indicare che la cosa: a) non deve essere *nullius* né *communis omnium*; b) non deve essere propria, cioè nella piena ed esclusiva signoria dell'agente.

fisica delle apparecchiature informatiche o telematiche, appariva invece estremamente problematico, alla luce del principio di legalità, pensare a un'inservibilità dell'apparecchiatura nell'ipotesi di una lesione dell'integrità della documentazione (dati o notizie) immessa nel calcolatore e non recuperabile in conseguenza dell'intervenuto danneggiamento, in mancanza di un contemporaneo danneggiamento del software. In questi termini, se non altro per motivi di chiarezza, l'intervento legislativo è sicuramente da apprezzare[198].

Nessun dubbio permane in tema di elemento soggettivo, in quanto, come nella fattispecie generale di danneggiamento, è richiesto il dolo generico, accogliendo tutti gli elementi costitutivi della fattispecie.

…Segue: la procedibilità a querela e la clausola di riserva

Preme, inoltre, soffermarsi sulla presenza della procedibilità a querela, relativamente al contenuto del comma 1°; essa infatti può certamente costituire un utile filtro per selezionare i fatti ritenuti meritevoli di criminalizzazione in concreto, alla stregua della volontà punitiva della persona offesa, perché la protezione penale dell'interesse di cui essa è titolare può essere lasciata alla sua libera disponibilità. Per tale ragione, si pone allora il problema di individuare con precisione chi sia da considerare persona offesa. Nel caso del delitto in esame, essa dovrebbe desumersi dal requisito dell'altruità dei dati danneggiati, ma, lo si è visto, non è affatto facile stabilirne la portata concreta. I dati, al pari delle informazioni e dei programmi, per la loro immaterialità non possono facilmente essere oggetto di possesso, come lo sono le cose e dunque non si può desumere da questo requisito quello negativo di altruità[199], come accade nei delitti contro il patrimonio, fra cui è collocato il danneggiamento comune (di cose) di cui all'art. 635. Sarà quindi necessario prendere come

[198] MARINI G., *Lineamenti del sistema penale*, Giappichelli, Milano, 2008, pag. 366.

[199] Nel caso di danneggiamento di "programmi" possono altresì essere considerate persone offese il concessionario e forse anche il legittimo utilizzatore, oltre che il concedente e proprietario; e potrebbero ancora esser tale l'operatore del sistema, legittimato agli interventi che subiscano pregiudizio dal danneggiamento stesso (si pensi a files di backup o di controllo, creati talora in modo molto complesso per determinate operazioni di manutenzione o aggiornamento, ecc.), nonché gli stessi partners commerciali o di lavoro di un'impresa o di un professionista, rispetto a dati ed informazioni non ad essi stessi riferibili, ma da essi forniti per determinate finalità operative, contrattuali, ecc.

riferimento il diverso ambito della legislazione in materia di protezione dei dati personali[200] e dovrà considerarsi: innanzitutto la figura dell'interessato definito come la persona cui i dati si riferiscono, quindi quelle del titolare nonché del responsabile del trattamento ovvero anche del sistema come tale, che ne è parimenti pregiudicato.

Per quanto invece concerne la clausola di riserva, essa opererà nel risolvere i rapporti di possibile interferenza con le nuove fattispecie di danneggiamento di sistemi e di dati di pubblica utilità nonché con riferimento ad eventuali altri delitti, come ad es. quelli di falsità per soppressione (ex artt. 476, 485 e 490) e, soprattutto, i reati contro la privacy (*in primis*, il già analizzato art. 167, 2° co., D.Lgs. 30.6.2003, n. 196).

…Segue: le circostanze aggravanti

Infine, opportuna appare la modifica del 2° comma dell'art. 635 bis c.p., rispondente alla necessità di porre rimedio, con l'occasione della ratifica della Convenzione Cybercrime , alla svista del legislatore del 1993, che aveva indiscriminatamente richiamato, come circostanze aggravanti speciali comportanti la pena della reclusione da uno a quattro anni, tutte quelle di cui al secondo comma dell'art. 635, oltre a quella nuova e specifica dell'essere il fatto commesso con abuso della qualità di operatore del sistema. Ferma quest'ultima ipotesi, è rimasto ora solo il richiamo al n. 1 di quelle di cui al capoverso dell'art. 635, riguardante la commissione del fatto "con violenza alla persona o minaccia", perseguibile d'ufficio, mentre sono state escluse tutte le altre ipotesi[201].

L'art. 635 ter

Passando ora al reato di cui all'art. 635 ter c.p.[202], rubricato " Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro

[200] Ai sensi del già analizzato decreto legislativo 196/2003.

[201] In questo senso si veda PICOTTI L., *La ratifica della convenzione cybercrime del consiglio d'Europa,* in *Diritto penale e processo*, 2008, 6, pag. 696.

[202] [1] Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.
[2] Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

ente pubblico o comunque di pubblica utilità", esso fu introdotto dalla legge 49/2008 che ha comportato la contestuale *abrogatio* del similare art. 420 c.p. comma 2° e 3°, concernente gli attentati ad impianti di pubblica utilità. Tuttavia, come si è detto in dottrina, non può parlarsi di una vera e propria abrogazione bensì di una continuazione normativa riformulando tali disposizioni, che pur contestualmente introducono ipotesi di reato, soprattutto aggravate, sostanzialmente nuove, pur mantenendo la stessa comminatoria edittale di pena[203]. Conseguentemente, quindi, la nuova fattispecie riprende e colloca la previsione dell'art. 420, 2° comma, scorporando tuttavia dall'originale incriminazione gli elementi di "dati, informazioni o programmi informatici", essendo gli altri "sistemi informatici o telematici", oggetto del successivo delitto di cui all'art. 635 quinquies, in conformità con la Convenzione Cybercrime che ha richiesto l'incriminazione distinta delle due ipotesi di danneggiamento di dati e di danneggiamento di sistemi[204]. Inoltre sono state riformulate le condotte punibili, venendo mantenuto solo il verbo "distruggere" mentre invece è stato soppresso il verbo "danneggiare" che invece compariva nell'art. 420, 2° comma integrando invece i verbi "cancellare, alterare o sopprimere" per conformare l'incriminazione a quanto richiesto dalle fonti sovranazionali.

Questo reato si colloca tra i delitti contro il patrimonio mediante violenza alle cose o alle persone, abbandonando definitivamente la precedente collocazione tra i delitti contro l'ordine pubblico dell'art. 420 essendo quindi evidente il profilo patrimonialistico di tale fattispecie, nonché la relativa idoneità a ledere l'integrità di risorse essenziali per l'azione pubblica. Eppure sembra corretto riproporre lo stesso pensiero individuato in tema di art. 635 bis per cui, almeno trasversalmente, deve comunque ritenersi coinvolto il bene giuridico della

---

[3] Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

[203] RESTA P., *Cybercrime e Cooperazione Internazionale nell'ultima legge della legislatura*, in *Giurisprudenza di Merito*, 2008, pag. 5.

[204] Come del resto rileva, PICOTTI L., *La ratifica della convenzione cybercrime del consiglio d'Europa*, in *Diritto penale e processo*, 2008, 6, pag. 714.

privatezza, come nel caso dell'alterazione di dati sensibili che fossero lecitamente utilizzati dallo Stato o altro ente pubblico.

Il delitto di danneggiamento di dati di pubblica utilità, al pari di quello previsto all'art. 635 quinquies, è formulato come un delitto di pericolo (di cui si nota la struttura tipica "fatti diretti a"), dal momento che la consumazione è anticipata già al momento della commissione di un fatto diretto a porre in essere le opere descritte nella norma, senza quindi che sia necessaria la loro effettiva realizzazione [205] . Lo svantaggio che, tuttavia, discende da una formulazione di questo tipo è che le condotte normative risulteranno eccessivamente evanescenti e di difficile percezione, al punto tale da causare situazioni di confusione rispetto alle condotte previste dall'art. 635 bis.

Per quanto concerne le aggravanti indipendenti che rendono la fattispecie un "delitto aggravato dall'evento", esse vengono individuate non solo nella distruzione delle informazioni, dei dati e dei programmi, ma anche nella cancellazione, nell'alterazione o nella soppressione degli stessi. Tra l'altro, data la formulazione della norma ("se dal fatto deriva...") e dall'entità della pena (stabilita in modo indipendente rispetto al 1° co.) si può desumere che si tratti di fattispecie autonome di reato[206] e non di mere circostanze aggravanti, con conseguente esclusione del bilanciamento tra circostanze ex art. 69 c.p.

Inoltre, all'art. 635 ter, 3° comma, si è introdotta un'ulteriore circostanza aggravante ad efficacia comune, applicabile tanto alle ipotesi del 1° quanto a quelle del 2° comma, caratterizzata dalla commissione del fatto con violenza o con minaccia alla persona o con abuso della qualità di operatore del sistema.

Infine, per quanto concerne gli ulteriori elementi della fattispecie, l'elemento soggettivo è, nuovamente, caratterizzato dal dolo generico, mentre per quanto riguarda il tentativo, esso è da escludere, pena l'arretramento sconsiderato della tutela penale di fronte ad un reato di pericolo.

---

[205] Anche se, comunque, il secondo comma prevede che nel caso di realizzazione dell'evento, la pena edittale consista nella reclusione da 3 a 8 anni.

[206] In questo senso anche PICOTTI L., *cit,* pag. 715.

L'art. 635 quater

L'art. 635 quater c.p.[207], rubricato "Danneggiamento di sistemi informatici o telematici", prevede un autonomo e più grave delitto rispetto all'art. 635 bis che tutela, invece, solamente informazioni, dati e programmi. Il 2° comma, invece, prevede una circostanza aggravante di formulazione pressoché identica a quella dell'art. 635 bis, 2° comma di cui *supra*, punita, però, con un aumento di pena non specificato[208].

Anche qui, come nell'articolo precedente, si ripropone la contrapposizione con l'art. 420, infatti, le principali differenze rispetto all'abrogata similare fattispecie riguardano in primo luogo l'oggetto materiale (ossia i "sistemi informatici o telematici altrui" anziché "dati, informazioni e programmi informatici altrui"), nonché una più ampia e articolata descrizione delle modalità di realizzazione della condotta, con conseguente maggior selettività della norma. Infatti, precedentemente, la fattispecie era a forma libera, mentre nella formulazione attuale essa si configura come un delitto a forma vincolata, incentrato sulla determinazione dell'inservibilità del sistema ovvero sul grave ostacolo frapposto al suo funzionamento.

Il reato è ora realizzabile tanto mediante quelle descritte nell'art. 635 bis quanto attraverso l'introduzione o la trasmissione di dati, informazioni o programmi e ciò è indice evidente di un'esigenza di punire le ulteriori ipotesi (immissione e trasmissione di dati) previste dall'art. 5 della Convenzione Cybercrime, al fine di colpire i danneggiamenti realizzabili a distanza, ossia mediante programmi virus o dati maligni introdotti nella rete (*trojan horses* e *logic bombs*) e in grado di rendere in tutto o in parte inservibili i

[207] [1] Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635 bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.
[2] Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

[208] In questi casi, tuttavia, va ritenuto che detto aumento, ai sensi della regola generale enunciata dall'art. 64 c.p., debba esser pari a un terzo della pena; ciò comporta che detta aggravante non sia classificabile quale circostanza speciale ex art. 63, 3° comma. Però, nel caso di specie, si è detto che la peculiarità di questa norma induce a pensare che il legislatore non abbia considerato le conseguenze sistematiche dei propri interventi ma, al contrario, che si sia limitato ad un'azione settoriale e limitata (PICOTTI L., *La ratifica della convenzione cybercrime del consiglio d'Europa*, in *Diritto penale e processo*, 2008, 6, pag. 712).

sistemi informatici o telematici altrui[209]. Tale ulteriore precisazione, oltre a recepire direttamente le indicazioni della Convenzione dimostra la particolare attenzione che il legislatore ha voluto riservare a quelle condotte particolari che si risolvono proprio nella diffusione di ogni possibile tipologia di virus informatico. Peraltro, bisogna rilevare che, sempre rispetto al contenuto dell'art. 420, debbono ritenersi abrogate le condotte, volte a rendere inservibili (in tutto o in parte) sistemi informatici o telematici altrui, realizzate con modalità diverse da quelle espressamente tipizzate[210]; si è dunque in presenza di *un'abrogatio cum abolizione criminis*, con conseguente applicabilità del regime di cui all'art. 2 c.p., 2° comma. Inoltre l'art. 635 quater, a ben vedere, mediante la locuzione "ostacola gravemente il funzionamento", intende ricomprendere anche le ipotesi non menzionate espressamente a livello nazionale ma previste in sede comunitaria (ad esempio "immissione", "trasmissione di dati", "interruzione"): ciò appare di estrema utilità se si guarda alle concrete modalità mediante cui vengono attaccati i siti o i portali, in tali vicende infatti normalmente l'attacco consiste nel rendere irregolare e frammentario il funzionamento dei sistemi e dei servizi cui i medesimi sono destinati.

Proseguendo con gli elementi costitutivi della fattispecie, deve evidenziarsi che tutte le condotte sin qui esaminate tipizzano in realtà un delitto d'evento, realizzabile attraverso qualsiasi modalità e che trova il suo momento consumativo nel prodursi dell'evento, in esecuzione della volontà dell'agente. Questo perché, nonostante vi sia un richiamo all'art. 635 bis, esso è riferito alle condotte e non all'intero comma 1°, motivo per cui non verrà presa in considerazione la dizione di "fatti diretti a" (che porterebbe ad un reato di pericolo), bensì solamente le condotte ivi coinvolte[211].

---

[209] AMATO G., *Danneggiamento perseguibile a querela*, in *Guida al diritto*, 2008, 16, pag. 61.

[210] C'è da dire, tuttavia, che quest'ultima ipotesi, invero, stanti le numerose modalità di realizzazione della condotta, appare decisamente marginale, se non addirittura residuale.

[211] C'è da dire, tuttavia, come rileva tra l'altro il PICOTTI, che, soprattutto in tema di reati informatici con condotte di questo tipo, risulti talvolta difficile individuare una precisa distinzione tra i concetti di condotta ed evento. Anche la condotta che si svolga con tecniche o strumenti informatici è infatti, per

L'art. 635 quinquies

A conclusione della trattazione in tema di reati informatici contro il patrimonio, caratterizzati da risvolti in tema di riservatezza, permane l'art. 635 quinquies c.p. [212], rubricato "Danneggiamento di sistemi informatici o telematici di pubblica utilità". Le considerazioni precedentemente sviluppate sulla struttura dei reati di evento e, quindi, sul momento consumativo dei delitti di danneggiamento di dati (art. 635 bis) e di sistemi informatici (art. 635 quater), trovano conferma sistematica, e anche rilievo pratico, nell'esame della fattispecie in oggetto, formulata come delitto di attentato in quanto la consumazione è anticipata già al momento della commissione di "un fatto diretto a" senza quindi che le ipotesi descritte si realizzino compiutamente. Inoltre, con struttura assolutamente speculare a quella dell'art. 635 ter, l'art. 635 quinquies si allinea alla formulazione di cui all'art. 635 quater, per quanto attiene all'enunciazione dei verbi "distruggere, danneggiare, rendere inservibile, ostacolarne gravemente il funzionamento". Maggiormente controversa è, invece, l'esatta definizione di aver "ostacolato gravemente il funzionamento di sistema informatico". In effetti si tratta di condotta che non sempre può essere facilmente apprezzabile (imponendosi, per forza di cose, una valutazione prognostica degli esiti di una condotta che non ha prodotto *in toto* gli effetti dannosi cui era indirizzata), almeno con riguardo alla fattispecie di pericolo di cui al 1° comma dell'articolo in esame, laddove viene punita quella sostanziatasi nella commissione di un fatto "diretto a" ostacolare gravemente il funzionamento del sistema informatico. Eppure secondo certa

---

sua natura, in tutto o in parte automatizzata, dovendo coinvolgere un "trattamento informatico" che cioè si svolge secondo un programma, come si ricava dalla definizione normativa di cui all'art. 1, lett. a, della Convenzione. Nel momento quindi in cui si manifesta nei rapporti sociali, con la vittima o con terzi anche indeterminati, può non essere agevole distinguere tale condotta "informatizzata" dagli effetti di modificazione della realtà oggettiva, che autonomamente determini quale sua conseguenza causale.

[212] [1] Se il fatto di cui all'articolo 635 quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.
[2] Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.
[3] Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

dottrina[213], la previsione sembra trovare una spiegazione, nel richiamo alle indicazioni alla Convenzione già più volte ricordata, dove l'attentato all'integrità del sistema informatico viene costruito attribuendosi rilievo a ogni condotta che si sostanzia in un serio ostacolo al funzionamento del sistema, anche quando questo, di fatto, non viene completamente danneggiato o reso inservibile. Si noti, inoltre, che a differenza di quanto avviene nella speculare ipotesi del 635 ter[214], nel primo comma in esame si fa riferimento esclusivamente alla sintetica locuzione "di pubblica utilità", identica peraltro a quella che compariva nell'abrogato 2° comma dell'art. 420. Si ritiene che questa nozione più generale appaia maggiormente idonea ad abbracciare tutte le situazioni ove il soggetto offeso sia lo Stato piuttosto che un Ente pubblico, non richiedendo come condizione necessaria l'utilizzazione effettiva da parte di un soggetto pubblico.

Circa l'elemento soggettivo è, nuovamente, richiesto il dolo generico e, per quanto concerne il tentativo, deve riprendersi la stessa posizione condivisa in tema di art. 635 ter.

Per quanto riguarda invece, le circostanze aggravanti, valgono le medesime considerazioni svoltesi circa l'artt. 635 ter e 635 quater, dalle quali esse sono mutuate.

[213] AMATO G., *cit*., pag. 61.

[214] Dove si utilizza sin dalla rubrica la complessa locuzione "sistemi informatici utilizzati dallo Stato o da altro Ente pubblico".

2.6 Frode informatica e «phishing»: premessa e ratio della norma (art. 640 ter)

L'articolo 640 ter c.p.[215] rappresenta una delle norme più interessanti in materia di *computer crimes*, in quanto in essa convogliano aspetti classici del diritto penale, quale lo schema della truffa ex. art. 640, e risvolti informatici particolarmente controversi, i quali hanno motivato il legislatore a dar vita alla fattispecie in esame. Essa nasce, come per gli altri delitti informatici, con la legge 547/93, tuttavia, con la Legge 119/2013, che converte il D.L. 93/2013, sono stati aggiunti i commi 3° e 4° in tema di furto di identità digitale.

La ratio della norma

Il motivo che ha spinto, *illo tempore*, il legislatore alla creazione di questo reato è stata l'effettiva difficoltà di ricondurre le ipotesi ora incriminate nell'ambito applicativo della truffa, pur ricalcandone il nuovo articolo lo schema[216]. Infatti, l'articolo 640 ter punisce le ipotesi di ingiusto profitto ottenuto mediante l'impiego alterato o senza diritto di un sistema informatico o telematico; prima dell'intervento modificativo del codice penale, risultava frutto di una forzatura ricondurre queste ipotesi alla fattispecie ex art. 640, dato che il divieto di analogia *in malam partem* non consentiva di assimilare l'operazione di intervento fraudolento sul funzionamento di una macchina alla condotta ingannevole verso un individuo persona fisica, propria della truffa.

Anche la giurisprudenza di legittimità si è espressa in tal senso, in quanto la norma in commento, pur ricalcando la fattispecie della truffa, non è ad essa perfettamente sovrapponibile. Riproposto lo stesso evento tipico, dice la Corte,

---

[215] [1] Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.
[2] La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.
[3] La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.
[4] Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o un'altra circostanza aggravante.

[216] In tal senso chiara la posizione di GAROFOLI R., *Manuale di diritto penale, parte speciale*, II, Roma, 2009, pag. 574.

l'aggressione al patrimonio viene descritta dall'art. 640 ter attraverso una diversa connessione eziologica tra le fasi che la realizzano, mancando poi il riferimento all'induzione in errore della vittima che presuppone un rapporto relazionale ed interpersonale fra soggetto agente e soggetto ingannato impossibile da riprodursi nel caso in cui l'atto di disposizione patrimoniale dipenda da un macchinario tramite un'operazione automatica[217].

Il bene giuridico tutelato di carattere plurioffensivo

Per quanto riguarda la sua sistemazione nel Codice Penale, la frode informatica è inserita nel capo dei "delitti contro il patrimonio mediante frode", ragion per cui il bene che il legislatore del 1993 ha voluto tutelare, quantomeno a livello primario, è il patrimonio. Tuttavia, in dottrina si è fatto strada un secondo orientamento tra coloro che ritengono che oggetto di tutela sia anche il regolare funzionamento dei sistemi informatici e, soprattutto, la riservatezza che ne deve accompagnare l'utilizzazione[218]. Infatti, sempre relativamente alla privacy dei soggetti coinvolti, la più recente giurisprudenza si è così pronunciata: "*Il bene giuridico tutelato dal delitto di frode informatica non può essere iscritto esclusivamente nel perimetro della salvaguardia del patrimonio del danneggiato, come pure la collocazione sistematica lascerebbe presupporre, venendo chiaramente in discorso anche l'esigenza di salvaguardare la regolarità di funzionamento dei sistemi informatici - sempre più capillarmente presenti in tutti i settori più importanti della vita economica, sociale, ed istituzionale del Paese - la tutela della*

---

[217] "*Il reato di frode informatica ha la medesima struttura, e quindi i medesimi elementi costitutivi, della truffa, dalla quale si distingue solamente perché l'attività fraudolenta dell'agente investe non la persona, bensì il sistema informatico (significativa è la mancanza del requisito della "induzione in errore" nello schema legale della frode informatica, presente invece nella truffa)* ". così C., Sez. IV, 4.10.1999 n. 3065 e, nello stesso senso, più recentemente, C., Sez. VI, 5.2.2009 n.8755.
Tuttavia, secondo una dottrina invero minoritaria, si è ritenuto che tale elemento sarebbe da ritenersi implicito, così da garantire alla norma sulla frode informatica di operare in un ambito circoscritto ad ipotesi nelle quali sarebbe stata applicabile la norma sulla truffa, se solo la condotta fraudolenta avesse interessato un individuo piuttosto che un computer (PECORELLA G., *Il diritto penale dell'informatic*a, 1996, Padova, pag. 51).

[218] In questo senso si ricorda autorevole dottrina fra cui ANTOLISEI F., *Manuale di Diritto Penale – Parte speciale I,* Milano, Giuffrè Editore, 2008, pag. 386 e FIANDACA G., MUSCO E., *Diritto penale Parte speciale II,* Zanichelli, Bologna, 2012, pag. 198. Vi è inoltre un terzo orientamento, minoritario, che considera incluso nella tutela anche il bene della libertà negoziale (PICA G., *Diritto penale delle tecnologie informatiche*, 1999, pag. 151; MASI G., Frodi *informatiche e attività bancaria*, in *Rivista di politica economica*, 1995, pag. 428).

riservatezza dei dati, spesso sensibili, ivi gestiti, e, infine, aspetto non trascurabile, la stessa certezza e speditezza del traffico giuridico fondata sui dati gestiti dai diversi sistemi informatici. Un articolato intessersi, dunque, di valori tutelati, tutti coinvolti nella struttura della norma, che indubbiamente ne qualifica, al di là del tratto di fattispecie plurioffensiva, anche i connotati di figura del tutto peculiare, e quindi 'speciale', nel panorama delle varie ipotesi di 'frode' previste dal codice e dalle varie leggi di settore"[219].

Dal nostro punto di vista, questa posizione è da condividere, ragion per cui il reato di frode informatica debba necessariamente configurarsi come un reato plurioffensivo che investa, oltre al patrimonio, anche il bene giuridico della riservatezza informatica. Inoltre, una posizione di questo tipo, come si vedrà di seguito, è anche supportata dall'introduzione dei commi 3° e 4°, in materia di furto dell'identità digitale, aspetto che, se possibile, ancor più si lega al concetto della privatezza informatica che il singolo desidera vedere protetta[220].

[219] Cass. pen. Sez. II, 15/04/2011, n. 17748.

[220] Si aggiunge, al discorso, una ulteriore posizione, per la quale vedendo Cass. sez. V. 24 novembre 2003, Noto, in *Giurisprudenza Italiana*, 2004, II, c. 2363, con nota di FERRARI, si è detto che il bene giuridico del reato in esame ricomprende il diritto del titolare del sistema informatico a godere liberamente e senza illecite intrusioni o manipolazioni dello stesso nonché dei diritti, anche non strettamente patrimoniali, che a mezzo del computer possono essere compromessi in maniera totale o parziale.

2.6.1 La struttura del reato e le modalità di condotta

Venendo alle modalità di condotta, essa è sostanzialmente uguale a quella del reato di truffa consistendo nel "procurare a sé o ad altri un ingiusto profitto con altrui danno", mentre differiscono le modalità di realizzazione del vantaggio economico che, mentre nella tradizionale ipotesi sono racchiuse nell'inciso "con artifici e raggiri, inducendo taluno in errore", nella frode informatica sono indicate in tassative modalità, "alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico" o "intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti"[221].

Alternatività delle condotte?

Una prima considerazione va svolta circa l'utilizzo della congiunzione "o" che lega i due periodi e che sembrerebbe implicare l'alternatività tra le due condotte che, poste in essere anche separatamente, provocherebbero entrambe l'insorgere di una condotta illecita integrante il reato. In realtà, in dottrina[222] si è osservato che tra queste ipotesi non vi sarebbe una netta distinzione, dal momento che la seconda condotta ricade da un punto di vista logico e tecnico nella prima, della quale costituirebbe una mera specificazione, proprio perché l'intervento si configurerebbe come un'operazione propedeutica all'alterazione del funzionamento della macchina. Tuttavia, *contra,* si pone certa giurisprudenza, la quale tende a riconoscere autonomia al concetto di intervento rispetto alla alterazione[223]. La norma, quindi, dovrebbe prevedere due distinte condotte: la prima consiste nell'alterazione, in qualsiasi modo, del funzionamento di un sistema informatico o telematico; la seconda è rappresentata dall'intervento senza diritto con qualsiasi modalità su dati,

[221] Conseguentemente potrebbe dirsi che tale nuova figura di reato dunque prevede due differenti ipotesi (alterazione ed intervento) che rappresentano gli artifici o i raggiri propri della frode informatica, in quanto modificano il funzionamento del sistema telematico o informatico per compiere operazioni che portano a risultati non voluti dal suo titolare ma vantaggiosi per l'agente.
[222] In questo senso si veda, PICA G., *Diritto penale delle tecnologie informatiche*, UTET, 1999, pag. 144.
[223] T. Milano 19.3.2007.

informazioni o programmi contenuti in un dato sistema informatico o telematico[224].

L'alterazione

L'alterazione si ritiene possa ottenersi in due maniere: o agendo sul software, la componente logica del computer, cioè su programmi, dati, informazioni installati e memorizzati in un apparato con capacità di elaborazione; ovvero operando sull'hardware, cioè sulle parti elettroniche, meccaniche, magnetiche, ottiche che ne consentono il funzionamento, in modo tale da far compiere operazioni diverse rispetto a quelle per le quali l'elaboratore è stato programmato. Similmente, la Corte di Cassazione, nella medesima sentenza del 2013, definisce per alterazione del funzionamento di un sistema informatico o telematico *"ogni attività o omissione che, attraverso la manipolazione dei dati informatici, incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei dati e, quindi, sia sull'hardware che sul software"*[225].

L'intervento

Per quanto invece riguarda l'"intervento su dati, informazioni o programmi", con esso deve intendersi ogni azione che produca una qualche modifica ai regolari processi dell'elaboratore. Come si ha avuto modo di vedere *supra*, per "dati" si devono intendere le registrazioni elementari nella memoria di una macchina elaboratrice codificate in una forma non percettibile visivamente e con "informazioni", intese come contenuto del sistema informatico, ci si riferisce ad un insieme più o meno vasto di dati organizzati secondo una logica che consenta di attribuire loro un particolare significato per l'utente della macchina. I programmi, invece, altro non sono se non sequenze di istruzioni. L'intervento sui programmi si compie facendo svolgere al computer operazioni in modo diverso da quelle programmate (ad esempio cambiando la funzione

[224] Qui, invece, la Corte di Cassazione Sez. II, 6 marzo 2013, n. 13475.

[225] Per altro, lo si è detto prima, antecedentemente all'introduzione dell'art. 640 ter, le condotte oggi previste da tale norma venivano fatte rientrare dalla giurisprudenza nell'ipotesi della truffa, come accaduto nel caso in cui il tribunale di Roma ha ritenuto integrato tale delitto nei confronti dell'INPS con riferimento condotta di alcuni soggetti che avevano immesso nel sistema informatico dell'istituto dati falsi relativi ai contributi previdenziali, ravvisando l'induzione in errore nei confronti dei funzionari preposti al controllo sul sistema informatico (T. Roma 20.6.1985; nello stesso senso, C., Sez. VI, 6.3.1989).

dei tasti di addizione e di sottrazione), così come si era inteso per le altre norme quali gli artt. 635 bis e ter[226].

L'espressione "senza diritto"

Per quanto riguarda l'espressione "senza diritto", se intesa letteralmente, essa dovrebbe significare due cose: assenza del consenso del titolare dei dati, informazioni e programmi contenuti nel sistema informatico quindi assenza del diritto di agire generalmente intesa, ma anche una modalità di azione *"non consentita da norme giuridiche, né da altre fonti"*[227]. Numerose sono state, altresì, le ulteriori posizioni dottrinarie su questo inciso. Per alcuni, tra cui Mantovani, dovrebbe trattarsi semplicemente di un'ipotesi di antigiuridicità speciale; per altri, tuttavia, esso invece appare ridondante ed inutile[228] o, addirittura, pericoloso, poiché "*vi è il rischio che si crei una sacca di impunità proprio tra gli addetti ai lavori*"[229]. Quest'ultima posizione, probabilmente la più convincente, si deve alla considerazione che, trattandosi di un reato volto al conseguimento di un ingiusto profitto a danno di altri, la posizione giuridica di chi utilizza in modo distorto il sistema informatico non dovrebbe rilevare; sarebbe perciò inutile determinare se l'agente abbia il diritto di intervenire sul sistema informatico o telematico, essendo sufficiente il fatto che l'intervento sia avvenuto con finalità illecite. Entrambe le condotte sono da ritenersi a condotta libera, come dimostrato dalle locuzioni utilizzate " in qualsiasi modo" o "con qualsiasi modalità". Pertanto, per il perfezionamento della fattispecie, non è richiesta alcuna specifica modalità di condotta.

---

[226] Una delle prime pronunce in materia ha ritenuto alterazioni rientranti in questa seconda ipotesi prevista dall'art. 640 ter le condotte criminose consistenti nell'effettuazione, attraverso apparecchi telefonici interni (Telecom di Brindisi) ed abilitati solo ad effettuare alcune chiamate interurbane, di chiamate internazionali verso l'Oceania e le Isole Cook attraverso la digitazione di una serie di numeri in grado di rendere inefficace il sistema di protezione di cui l'apparecchio telefonico è dotato. Il tribunale, partendo dal presupposto che il sistema Telecom potesse essere considerato "informatico", ha sostenuto che la condotta in esame costituisse un intervento indebito su dati contenuti nel sistema informatico (Cass. pen. Sez. VI, 4 Ottobre 1999, n. 3065).

[227] DESTITO V., DEZZANI G., SANTORIELLO C., *Il diritto penale delle nuove tecnologie*, Padova, 2007, pag. 43.

[228] ALMA-PERRONI, *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Diritto penale e processo*, 1997, pag. 506.

[229] PICA G., *cit,* pag. 146.

2.6.2 L'ingiusto profitto e l'altrui danno; l'elemento soggettivo, le circostanze aggravanti e i rapporti con altri reati

L'ingiusto profitto e l'altrui danno

Proseguendo secondo la lettera di questo delitto, per il perfezionamento del reato è richiesto che l'agente procuri a sé o ad altri un ingiusto profitto con altrui danno, configurandosi, in questo modo, proprio come per la truffa, come evento del reato. Conseguentemente si avrà il momento consumativo nel luogo di esecuzione della attività manipolatoria del sistema di elaborazione dei dati, che quindi può anche coincidere col conseguimento del profitto anche non economico[230].

Sul termine di profitto, si ritiene si possa intendere qualunque utilità, anche di natura non strettamente patrimoniale, per cui non è necessario che il profitto perseguito dall'agente abbia carattere economico, potendo esso consistere nel soddisfacimento di un bisogno di qualsiasi genere, anche soltanto psicologico o morale[231]. Dunque, in linea con questi orientamenti, può dirsi che col profitto non si debba intendere necessariamente una somma di denaro, potendo invece consistere in qualunque altro bene, purché suscettibile di valutazione economica e la cui sottrazione comporti all'offeso un danno [232] che, al contrario, deve sempre avere natura patrimoniale.

Per la giurisprudenza, ai fini dell'applicazione del 640 ter, si richiede che il profitto sia stato realizzato attraverso una ingiusta modalità di ottenimento, dovendosi intendere che il soggetto si sia mosso in un ambito di illiceità, che abbia cioè agito in posizione di contrarietà rispetto all'ordinamento giuridico traendo una utilità che non gli era dovuta per legge. Tuttavia questo

[230] Su questo punto molto chiara la sentenza di Cassazione sez. III del 24 maggio 2012 n. 23798, per la quale "*ai fini della determinazione della competenza territoriale, nel reato di frode informatica il momento consumativo va individuato nel luogo di esecuzione della attività manipolatoria del sistema di elaborazione dei dati, che può coincidere con il conseguimento del profitto anche non economico. (Fattispecie nella quale il luogo di commissione del reato è stato individuato nella sede della società gestita dagli imputati, presso la quale si trovavano i server contenenti i dati oggetto di abusivo trattamento)".*

[231] Diverse le sentenze che hanno da tempo segnato questo orientamento unitario: C., S.U., 6.12.1998; C., Sez. II, 14.4.1983; C., Sez. I, 3.11.1967; C., Sez. II, 20.6.1967; C., Sez. II, 21.4.1965.

[232] Che, secondo il MANZINI, viene tradizionalmente scomposto tanto nel danno emergente quanto nel lucro cessante. Il danno di cui si tratta deve provenire dalla privazione o menomazione di un diritto esistente e certo.

orientamento giurisprudenziale è stato criticato da alcuni autori, fra cui Antolisei, i quali hanno ritenuto che esso comporterebbe un eccessivo allargamento del campo di operatività della disposizione, poiché così argomentando vi rientrerebbero anche comportamenti finalizzati al conseguimento di un profitto non dovuto per legge, anche se non illeciti o contrari all'ordinamento giuridico. Il concetto di profitto *sine iure* è stato reso più comprensibile facendo l'esempio delle obbligazioni naturali "*le quali, come tutti sanno, se non autorizzano l'azione giudiziaria per l'adempimento, tuttavia escludono la facoltà di ripetere quanto sia stato spontaneamente prestato in esecuzione di esse*". Inoltre, come già accennato, la norma non menziona tra gli elementi costitutivi l'induzione in errore, come nella truffa, poiché l'alterazione dei dati informatici prescinde da qualsiasi inganno del sistema informatico o del suo titolare.

L'elemento soggettivo

Per quanto riguarda l'elemento soggettivo del reato di frode informatica, è richiesto il dolo generico avente ad oggetto tutti gli elementi costitutivi indicati dalla norma anche se preveduti dall'agente come conseguenze possibili della propria condotta. Ciò vuol dire che il reato in esame è compatibile anche col dolo eventuale, cioè quella forma di dolo che si caratterizza per una minor intensità e gravità per la quale l'evento costituente reato non è voluto direttamente dal soggetto, ma comunque previsto come conseguenza della sua condotta, agendo il reo a costo di determinare tale evento[233].

Le circostanze aggravanti: a danno dello Stato o di altro ente pubblico

Venendo ora alle circostanze aggravanti, in presenza delle quali il reato è procedibile d'ufficio, al comma 2° sono previste due ipotesi. La prima tratta il caso in cui la frode informatica sia commessa a danno dello Stato o di altro ente pubblico o col pretesto di fare esonerare taluno dal servizio militare, con un espresso richiamo a quanto stabilito dall'art. 640, 2° comma n. 1; una recente sentenza di Cassazione ha stabilito che, tra la frode informatica

[233] Circa l'ammissibilità del dolo eventuale per l'articolo 640 ter si veda AMATO G., DESTITO V. S., DEZZANI G., SANTORIELLO C., *I reati informatici,* CEDAM, Padova, 2010, pag. 110.

aggravata a danni dello Stato e peculato, l'elemento distintivo è costituito dalle modalità di possesso del denaro o d'altra cosa mobile altrui oggetto di appropriazione, ricorrendo il reato di peculato se il pubblico ufficiale o l'incaricato di pubblico servizio se ne appropri avendone già il possesso o comunque la disponibilità per ragione del suo ufficio o servizio, ricorrendo, al contrario, la frode informatica allorché il soggetto agente, non avendo tale possesso, se lo procuri fraudolentemente, facendo ricorso ad artifici o raggiri per procurarsi un ingiusto profitto con altrui danno[234] [235].

L'abuso della qualità di operatore di sistema

La seconda ipotesi prevede, invece, il caso in cui la frode informatica sia commessa abusando della qualità di operatore del sistema. Questa ipotesi è stata da molti giustificata a causa della maggiore facilità di intervento che tale mansione offre al soggetto agente, il che fa sì che quest'ultimo sia connotato da "*una particolare pericolosità sociale in considerazione del suo rapporto privilegiato con il sistema*"[236]: dati, programmi ed informazioni risulteranno in relazione a questo soggetto ancora più vulnerabili. Quest'aspetto è stato anche recentemente sottolineato dai giudici di legittimità in un caso in cui un soggetto, dopo essersi appropriato della password rilasciata ad un terzo, responsabile di zona di una compagnia assicurativa, manipolava i dati del sistema, predisponendo false attestazioni di risarcimento dei danni[237].

In questo modo, abusando della propria posizione, l'operatore viola un dovere di fedeltà cui è tenuto sia nei confronti del titolare del sistema informatico a lui delegato, sia delle persone i cui interessi economici sono presi in carico da quel sistema. Tuttavia, resta controverso cosa debba intendersi esattamente per

---

[234] In questo senso Cass. Pen., Sez. II, 10.4.2013, n. 18909.

[235] Inoltre, sempre per questa prima ipotesi, l'art. 640 quater prevede come obbligatoria la confisca dei beni che costituiscono il prezzo o il profitto del reato. Ci si è chiesti se lo stesso valga per l'ipotesi in cui sussistono cumulativamente entrambe le aggravanti. A questo interrogativo ha provveduto a rispondere la giurisprudenza di legittimità che ha risolto la questione nel senso che la confisca dovrà escludersi nel caso in cui ricorra la sola circostanza aggravante dell'abuso della qualità di operatore del sistema, dovendo invece essere applicata qualora tale aggravante concorra con quella di cui all'art. 640, 2° co., n. 1 (così Cass. pen. Sez. VI, 11/03/2009, n. 16669).

[236] BUONOMO G., *Metodologia e disciplina delle indagini informatiche*, in BORRUSO-BUONOMO-CORASANITI-D'AIETTI, *Profili penali dell'informatica*, Giuffrè, Milano, 1994, pag. 39.

[237] C., Sez. II, 11 novembre 2009 n.44720.

operatore del sistema, essendo questa espressione vaga e non definita da alcuna fonte legislativa. Probabilmente, per identificare cosa il legislatore abbia voluto intendere è essenziale fare riferimento alla *ratio* della norma, cioè alla necessità di punire ancora più incisivamente coloro che, approfittando delle proprie personali competenze, abbiano cagionato un danno ad altri traendone profitto ingiustamente[238].

L'aggravante del furto digitale

Infine, come anticipato *supra*, la terza ipotesi aggravante, introdotta dalla Legge 119/2013, fa riferimento all'ipotesi della commissione del fatto con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti, che sarà approfondita in dettaglio nel prossimo paragrafo.

La norma mira a contrastare il sempre più diffuso fenomeno delle frodi realizzate attraverso l'accesso abusivo a un sistema informatico con l'indebito utilizzo dell'identità digitale altrui. Il testo originario del decreto legge faceva riferimento alla "*sostituzione dell'identità digitale*", espressione ritenuta ambigua, poiché "*formalmente evoca, piuttosto che l'indebito utilizzo dell'identità, la sua surrogazione con altra al fine di accedere ai dati raggiungibili con quella sostituita e cioè fattispecie diversa e ben più specifica di quella ipotizzata in precedenza, ma di dubbia rilevanza*" [239]. La legge di conversione ha modificato la disposizione, facendo esplicito riferimento al furto e all'indebito utilizzo dell'altrui identità digitale, purché commessi in danno di uno o più soggetti.

---

[238] In dottrina, vi è stato chi ha sostenuto che per operatore del sistema debba intendersi qualsiasi tecnico legittimato ad operare sul computer (BORRUSO in BORRUSO, BUONUOMO, CORASANITI, D'AIETTI, cit, pag. 27) e chi, in senso opposto, ha invece considerato la posizione del tecnico che abbia il controllo su varie fasi di elaborazione dei dati, escludendo sia del semplice operatore addetto a funzioni meramente esecutive sia del programmatore che possiede solo una conoscenza settoriale dei dati relativi alla macchina (POMANTE, *Internet e criminalità*, Torino, 1999, pag. 11). Per una interpretazione più funzionale, pare debba adottarsi una soluzione mediana, intendendo che il legislatore abbia voluto considerare la posizione di tutti i soggetti che possono legittimamente operare sul sistema e che godono delle qualifiche professionali o di conoscenze specifiche rispetto a quelle di un qualsiasi altro operatore del sistema (MUCCIARELLI G., *Commento all'art.10 della legge 547 del 1993*, in *L'indice penale*, 1996, pag. 102).

[239] Così ritiene PISTORELLI, *Relazione dell'Ufficio Massimario della Corte di Cassazione*, n. III/1/2013.

Il rapporto con altri reati

Per quanto riguarda invece i rapporti con altre figure criminose, bisogna *in primis* rilevare che deve ritenersi sussistente il reato di truffa e non quello di frode informatica tutte le volte in cui sia ingannata la persona offesa, seppure ciò avvenga avvalendosi di strumenti informatici o se l'atto di disposizione patrimoniale, da cui discende il profitto e il danno corrispondente, viene posto in essere in via telematica[240].

Inoltre, nella maggior parte dei casi, il reato in esame verrà in essere unitamente ad altri delitti informatici solitamente prodromici alla realizzazione della frode informatica[241], quali accessi informatici abusivi (art. 615 ter), detenzione o diffusione di codici di accesso a sistemi informatici (art. 615 quater), diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere sistemi informatici (art. 615 quinquies) oppure danneggiamenti informatici di cui agli artt. 635 bis e seguenti che concorreranno con la frode per via dei diversi beni giuridici tutelati. Sicuramente il concorso di reati va ammesso fra quello *de quo* e quello ex art. 615 ter il quale, tutelando il domicilio informatico sotto il profilo dello *ius excludendi alios*, si differenzia dall'articolo 640 ter improntato invece, principalmente, all'alterazione dei dati immagazzinati nel sistema al fine della percezione dell'ingiusto profitto[242].

[240] Quindi dovranno tenersi ben distinti quei fatti, pur ricollegabili all'informatica, in cui vi è un induzione in errore dell'uomo da quelli ove vie è un'alterazione o un intervento non consentito sul sistema informatico. Solo in questo caso ricorrerà il reato di frode informatica e, dunque, non potrà ravvisarsi il concorso formale con la truffa in ragione della specificità della frode informatica.

[241] E, dunque, potrà ravvisarsi relativamente ai reati prodromici l'aggravante del nesso di connessione teleologica di cui all'art. 61 n.2 del Codice Penale.

[242] In questo senso si veda Cass., Sez. V, 30 settembre 2008, Romano, in *Mass. Ufficiale* 242938.

2.6.3 Il «phishing»: il significato e la recente sentenza di Cassazione n. 9891 del 2011

Cos'è il furto di identità digitale ed il phishing?

Una particolare modalità di frode informatica che negli ultimi anni ha avuto grande diffusione è quella denominata *phishing*[243]. Si tratta di un fenomeno di ingegneria sociale volto al furto d'identità che trae origine dall'invio casuale di messaggi di posta elettronica che riproducono la grafica e i loghi ufficiali di siti aziendali o istituzionali come quelli postali o bancari, ad un elevato numero di destinatari (essendo quindi una tecnica di *spamming*). Tali messaggi, di solito, segnalano all'utente presunti problemi tecnici relativi all'accesso al conto, inducendolo all'inserimento di password che autorizzano pagamenti o numeri di carte di credito.

Il comma 3°, come si è visto, ha rafforzato la tutela penale dell'identità digitale, inserendo l'aggravante alla frode informatica se effettuata tramite il furto di identità digitale, col quale si intende "*l'ipotesi in cui un soggetto acquisisce, trasferisce, possiede o utilizza informazioni personali di una persona fisica o giuridica in modo non autorizzato, con l'intento di commettere, o in relazione a, frodi o altri crimini*"[244].

La sostituzione di persona come antecedente normativo

Andando con ordine, prima della disposizione in esame, il caposaldo della tutela penale dell'identità personale era il reato di sostituzione di persona (art. 494 c.p.), il quale sanziona chi, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore sostituendo

---

[243] Il cui significato deriva dalla crasi dei termini inglesi di "*password*" e "*fishing*", vale a dire pesca di password. Nel dettaglio si veda CAJANI F.,*La tutela penale dell'identità digitale alla luce delle novità introdotte dal D.L. 14 agosto 2013, n .93 (convertito con modificazioni dalla L. 15 ottobre 2013, n.119),* in *Cassazione Penale, 3*, 2014, pag. 1094 e ss.

[244] Definizione fornita dall' Organizzazione per la cooperazione e lo sviluppo economico (OCSE) nell'importante documento *"Scoping Paper on Online Identity Theft"* del 2008: www.oecd.org/dataoecd/35/24/40644196.pdf a pag. 12. Quanto al panorama italiano, il legislatore, sia pure ai soli fini del d.lg. 13 agosto 2010, n. 141, ha dato la seguente nozione di "furto di identità":
"*a) l'impersonificazione totale: occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto. L'impersonificazione può riguardare l'utilizzo indebito di dati riferibili sia ad un soggetto in vita sia ad un soggetto deceduto; b) l'impersonificazione parziale: occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto, nell'ambito di quelli di cui alla lettera a)*".

illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici. Inoltre, a supporto del contenuto di questo reato, la Corte di Cassazione, con sentenza n.46674 del 2007, ha sancito il principio per cui tale reato sussiste anche se commesso in rete e, più precisamente, laddove venga creato fittiziamente a nome altrui un account di posta elettronica[245].

Proseguendo, c'è da dire, tuttavia, che la condotta illecita che integra il furto di identità digitale è spesso poi indirizzata alla realizzazione di ulteriori e ben più gravi offese nei confronti del malcapitato. Il *phishing* è, infatti, una classica ipotesi in cui al furto di identità digitale segue un concreto danno patrimoniale, che avviene quando, tramite invio da parte di ignoti truffatori di messaggi di posta elettronica ingannevoli, la vittima è spinta a fornire volontariamente informazioni personali sensibili o comunque riservate, come le password di accesso ai servizi di *home banking*[246], sfruttando i sovracitati metodi di *social engineering*[247], mancando quindi il vero e proprio attacco informatico tale da colpire il sistema informatico bancario. I messaggi propri del *phishing* segnalano, ad esempio, presunti problemi tecnici occorsi sul server della propria banca, oppure insoliti tentativi di accesso al conto o anche procedure di aggiornamento al sistema di identificazione; successivamente, per risolvere il problema, si richiede all'utente di inserire i propri dati sensibili accedendo ad una pagina web indicata nella mail che ha ricevuto, il tutto contornato da elementi allarmanti e minacciosi, quali il possibile blocco del conto corrente.

[245] Orientamento che non fu affatto isolato, ma fu riconfermato anche dalla sentenza di Cassazione n.12479 del 2011, secondo la quale commette il reato in esame "*chi apre e registra un account di posta elettronica a nome di un'altra persona, per poter partecipare alle aste online e far ricadere così sull'intestatario inconsapevole le conseguenze dell'inadempimento nelle obbligazioni di pagamento relative a tale acquisto*".

[246] Riprendendo le considerazioni di FLORA G., *Il furto di identità,* in AA.VV., *Sicurezza e privacy: dalla carta ai bit*, a cura di COSTABILE, Esperta Edizioni, 2005, pag. 237, il funzionamento della maggior parte dei servizi online è caratterizzato dall'accoppiata composta da un nome utente e una password la quale, solitamente, è conosciuta solo al al soggetto e al sistema e che conferma ad ogni effetto la dichiarazione di identità del nome utente, autorizzandolo all'accesso.

[247] Termine con cui si intende lo studio del comportamento individuale di una persona al fine di carpire informazioni. Un ingegnere sociale per definirsi tale, dovrà saper fingere, saper ingannare altri e quindi mentire. Egli nasconde la propria identità fingendosi altre persone cosi da ricavare informazioni che non potrebbe altrimenti ottenere con la sua reale identità: MITNICK, *L'arte dell'inganno*, Feltrinelli, 2003.

Nel momento in cui la vittima inserisce le credenziali ed il *phisher* le acquisisce, egli avrà, ovviamente, la piena possibilità di disporre bonifici online in frode al legittimo intestatario[248].

L'art. 640 comma 3° per la condotta di phishing

Dunque, nel caso in cui la condotta criminosa di furto di identità digitale sia accompagnata da ulteriori finalità illecite, come appena analizzato, si ritiene si possa rientrare all'interno dell'aggravante di cui all'art. 640 ter comma 3°. Con tale disposizione, può dirsi tranquillamente che, per la prima volta in Italia, sia rinvenibile il primo terreno normativo in relazione al fenomeno del *phishing.* Tuttavia, nel momento in cui è avvenuta tale modifica normativa, non sono mancati, in dottrina, i dubbi circa l'eventuale e ulteriore possibilità di far rientrare tale illecita condotta non solo all'interno dell'art. 640 ter comma 3°, ma anche nella più generale disposizione dell'art. 640 di truffa. Si era detto, infatti, che la tesi della configurabilità della truffa era da preferirsi in quanto l'elemento oggettivo della frode informatica richieda (come *quid pluris* rispetto all'art. 640), la necessaria realizzazione di una delle due condotte dell'art. 640 ter, di cui *supra,* che nel caso del *phishing* non sembrano essere richieste[249].

L'importanza della sentenza di Cassazione n.9681 del 2011

Eppure, ancor più di recente, è prevalsa una diversa impostazione che valorizza la condotta dell'utilizzo delle credenziali indebitamente acquisite dal *phisher* con un "*intervento non autorizzato su informazioni contenute in un sistema informatico*" proprio come previsto dall'art. 640 ter[250]. In questo senso si è infatti allineata la pronuncia dei giudici di legittimità n. 9681 del 2011, per la quale si è detto che nel reato in esame, l'utilizzazione della password, illecitamente ottenuta, per addentrarsi in un sistema informatico, tramite tecniche di *phishing*, possa pacificamente rientrare nella fattispecie delineata

[248] La sentenza del Tribunale di Milano del 10 dicembre 2007 rappresenta la prima condanna, in Italia, di membri di una associazione transnazionale dedita alla commissione di reati di *phishing*, riconfermata in Cassazione nel 2011. Essa, ovviamente, è anche la prima che cerca di rinvenire, nel panorama penale, le norme applicabili a questa particolare condotta criminosa.

[249] Si veda, per una spiegazione più dettagliata, CAJANI F., *Profili penali del phishing,* in *Cassazione Penale,* 2007, pag. 2299.

[250] CAJANI F., *La tutela penale dell'identità digitale alla luce delle novità introdotte dal D.L. 14 agosto 2013, n .93 (convertito con modificazioni dalla L. 15 ottobre 2013, n.119),* in *Cassazione Penale, 3*, 2014, pag. 1103.

dall'art. 640 ter comma 3°[251]. Tra i vantaggi che la Corte riconosce ad una posizione di questo tipo, sicuramente vi sono i limiti edittali più ampi (con una pena massima di 6 anni che consente anche il ricorso alle misure cautelari) e, soprattutto, la procedibilità d'ufficio. Concludendo, può dunque dirsi che, alla luce dei principi dettati dalla sentenza in esame, la nuova disposizione dell'art. 640 ter disciplini in modo più idoneo e completo il fenomeno del *phishing*, in quanto non c'è dubbio che, nella condotta subito successiva al furto di identità digitale, consistente nella realizzazione di false pagine di accesso bancario o inserzioni di vendita fittizie, possa concretizzarsi l'ipotesi di un intervento senza diritto sui dati e informazioni contenuti nel sistema informatico messo a disposizione dell'utente originario dai rispettivi sistemi informatici in questione. Per questo motivo, ben si comprende come la potenziale portata applicativa della norma recentemente introdotta sia effettivamente in grado di rafforzare la tutela penale della riservatezza e dell'identità digitale in ogni sua concreta lesione effettuata tramite la rete *Internet.* Probabilmente, il rafforzamento sarebbe stato anche più elevato se, come si vedrà nel capitolo che segue, non fosse venuta meno, con la legge di conversione, la previsione di una responsabilità amministrativa degli enti nei casi di commissione, ad opera di dipendenti o soggetti apicali del delitto di frode informatica mediante furto dell'identità digitale.

[251] Nel dettaglio la Corte ha ritenuto che: "*Nella fattispecie in esame, l'utilizzazione della password illecitamente ottenuta per entrare nel sistema informatico di home banking del correntista (protetto da misure di sicurezza costituite, appunto, dai dati di accesso personali) e messo a sua disposizione dalle Poste Italiane, servì per stornare fondi dal conto corrente della C.: con il che si è verificata l'ipotesi di intervento (nella specie: ordine di bonifico dal conto corrente della C. a quello dell'imputato) senza diritto sui dati e/o informazioni (nella specie: sul saldo attivo del conto corrente) contenuti nel suddetto sistema informatico. Si può quindi concludere ... che la fattispecie, così come contestata, rientra nell'ipotesi criminosa di cui all'art. 640-terc.p, atteso che i suddetti reati hanno diversi presupposti giuridici e, quindi, ben possono concorrere (in terminis Cass. 2672/2003 riv 227816; Cass. 1727/2008 riv 242938): non a caso, secondo quanto riferito dallo stesso ricorrente (pag. 3 ricorso), il reato di accesso abusivo al sistema informatico fu contestato ma dichiarato improcedibile per mancanza di querela*".

CAPITOLO V – I REATI A TUTELA DELLA PRIVACY E LA DISCIPLINA DELLA RESPONSABILITÀ DEGLI ENTI

1. La funzione del D.lgs 231/2001: "Responsabilità amministrativa da reato". Premessa e considerazioni generali - 2. Lineamenti essenziali della responsabilità delle persone giuridiche da reato; i modelli organizzativi e la tipologia delle sanzioni - 3. L'introduzione da parte della L. 48/2008 nel D.lgs 231/2001 dell'art. 24 bis rubricato "Delitti informatici e trattamento illecito di dati" - 4. Il D.L. 93/2013 e l'aggiunta dei reati privacy all'interno dell'art. 24 bis del D.lgs 231/2001; la loro mancata conversione con la L. 113/2013; de iure condendo: il Regolamento Europeo sui dati personali

1. *La funzione del D.lgs 231/2001: "Responsabilità amministrativa da reato". Premessa e considerazioni generali*

Il decreto legislativo dell'8 giugno 2001 n. 231 è stato il provvedimento normativo del Governo che ha dato attuazione alla delega conferita dall'art. 11 della legge n. 300 del 2000 per la disciplina della responsabilità amministrativa delle persone giuridiche e delle società, degli enti e delle associazioni prive di personalità giuridica che non svolgano funzioni di rilievo costituzionale[1].

L'importanza del D.lgs 231/2001 e il rapporto con i reati informatici

Con questo intervento si è, per la prima volta, introdotto nel nostro ordinamento una responsabilità delle persone giuridiche come conseguenza degli illeciti penali commessi da chi agisce in nome e per conto della società. In questo modo, ha preso strada, accanto alla tradizionale responsabilità penale di carattere esclusivamente personale, un'ulteriore responsabilità della persona giuridica totalmente divergente rispetto ai modi con cui l'ente, in precedenza, poteva essere chiamato a rispondere degli illeciti dei suoi dipendenti[2].

[1] La letteratura su questa disciplina è già amplissima, senza pretesa di completezza si citano: AA.VV., *Reati e responsabilità degli enti,* a cura di LATTANZI, Giuffrè, Milano, 2005; AA.VV. *La responsabilità da reato degli enti collettivi. Cinque anni di applicazione del d.lgs. 8 giugno 2001 n. 231,* a cura di SPAGNOLO N., Giuffrè, Milano, 2007; REVERDITI M., *La responsabilità degli enti: la crocevia fra responsabilità da reato degli enti collettivi*, Giuffrè, Milano, 2009.

[2] Si pensi alla responsabilità della persona giuridica civilmente obbligata per il pagamento della pena pecuniaria.

Dunque, è ora riconosciuta e disciplinata in via diretta una responsabilità penale della persona giuridica, sviluppando un apparato sanzionatorio che trova applicazione in via esclusiva nei confronti dell'ente, il quale non è più chiamato a rispondere solo in via sussidiaria in caso di inadempienza della persona fisica condannata. La necessità di costituire una responsabilità nuova nei confronti delle persone giuridiche nasce tanto dagli adempimenti agli obblighi europei e internazionali quanto da una forte elaborazione dottrinale sul tema in questione[3], la quale già aveva evidenziato l'inadeguatezza delle sanzioni previste dall'ordinamento per fronteggiare la criminalità d'impresa.

All'interno di questa parte dell'elaborato, si cercherà di analizzare il problematico rapporto che intercorre fra le fattispecie sopra analizzate, vale a dire, principalmente, i reati informatici in tema di riservatezza, e tale responsabilità penale delle persone giuridiche. Si avrà modo di vedere che non tutti i reati privacy sono presenti nel decreto 231, poiché, una parte di questi, è stata oggetto, *in primis*, di una conferma, tramite decreto legge e, successivamente, di un'abrogazione, in sede di conversione del decreto.

Responsabilità penale o amministrativa?

Tuttavia, prima di giungere al nucleo del discorso, è necessario fornire alcune precisazioni e delucidazioni in materia di responsabilità delle persone giuridiche; l'argomento è, infatti, assai dibattuto, a partire dalla natura giuridica che si attribuisce a tale responsabilità.

Nel testo normativo, questa particolare forma di responsabilità è, difatti, qualificata come amministrativa, eppure gran parte della dottrina contesta questa concezione, sostenendo che, invece, si è in presenza di una responsabilità penale a tutti gli effetti[4]. A favore di ciò deporrebbero alcuni aspetti quali: la connessione diretta di tale forma di responsabilità con la

[3] Anche qui, senza pretesa di completezza, si cita: ALESSANDRI A., *Reati d'impresa e modelli sanzionatori,* Giuffrè, Milano, 1984; FOGLIA MANZILLO V., *Verso la configurazione della responsabilità penale per la persona giuridica,* in *Diritto e procedura penale,* 2000, pag. 196; MARINUCCI G., "societas punir ipotest": *uno sguardo sui fenomeni e sulle discipline contemporanee,* in *Rivista italiana di procedura penale*, 2002, pag. 1193.

[4] In questo senso si veda CORDERO F., *Procedura Penale,* Giuffrè, Milano, 2003, pag. 1329; ZAGREBELSKY V., *La convenzione europea dei diritti umani, la responsabilità delle persone morali e la nozione di pena,* in AA.VV., *Responsabilità degli enti,* pag. 31.

realizzazione di un reato; la circostanza che la decisione è affidata alla competenza del giudice penale; la prevista autonomia della responsabilità *ex delicto* dell'ente, che persiste anche quando l'autore del reato non è stato identificato o non è imputabile o il reato è estinto per causa diversa dall'amnistia; i criteri di imputazione dell'illecito sul piano oggettivo; le finalità completamente special-preventive delle sanzioni interdittive, modellate su sanzioni di carattere penale.

Posizioni contrarie[5] ritenevano, tuttavia, che la conclusione circa la natura penale della responsabilità degli enti sarebbe contraddetta da altrettanti aspetti del sistema delineato dal decreto legislativo in esame. Infatti, oltre alla dizione assunta dal legislatore a titolo del decreto, vengono evidenziati alcuni elementi strutturali che farebbero propendere per una natura amministrativa piuttosto che penale; essi sono: il regime della prescrizione, fortemente slegato dai meccanismi penalistici; il trattamento sanzionatorio previsto nel caso di vicende modificative dell'ente, legato totalmente alla disciplina civilistica relativa alla traslazione delle obbligazioni della società oggetto della modifica; l'assenza di una disposizione che disponga il cumulo fra le sanzioni dell'ente e dell'autore del reato; la mancanza di un regime di conversione delle pene pecuniarie; l'inesistenza di istituti sospensivi nell'applicazione della sanzione.

Lo spostamento del problema sul piano costituzionale

Eppure, recentemente, la dottrina ha decisamente ridimensionato la rilevanza di questa problematica, anche nella consapevolezza delle difficoltà di aderire pacificamente all'una o all'altra soluzione, riconoscendo che, in un certo senso, sia la responsabilità penale che quella amministrativa sono figure inadeguate a "*ricevere l'innesto del nuovo istituto*"[6]. Pertanto, la riflessione dottrinaria si è spostata su un piano diverso, vale a dire se la responsabilità delle persone giuridiche non presti il fianco a censure di incostituzionalità

[5] ALESSANDRI A., *Riflessioni penalistiche sulla nuova disciplina,* In AA.VV., *Responsabilità d'impresa e strumenti internazionali anticorruzione,* a cura di SACERDOTI, Giuffrè, Milano, 2003, pag. 49; COCCO G., *L'illecito degli enti dipendenti da reato ed il ruolo dei modelli di prevenzione,* in *Rivista italiana di diritto e procedura penale,* 2004, pag. 116; RUGGIERO C., *Capacità penale e responsabilità degli enti,* Giappichelli, Torino, 2004, pag. 277.

[6] ALESSANDRI A., *cit.,* pag. 50.

nella parte in cui si puniscano condotte di soggetti privi di una propria individualità giuridica e, cioè, non portatori di una volontà colpevole ex. art. 27 Cost. La maggior parte della dottrina ha negato il fondamento di dubbio di incostituzionalità, sottolineando, piuttosto, come l'innovativo intervento del legislatore fosse invece idoneo ad affermare una nuova lettura del principio costituzionale della responsabilità personale. Infatti, per questa teoria, il decreto 231 fonderebbe la colpevolezza dell'ente sul fatto che tale soggetto avrebbe assunto, con i propri rappresentanti o dipendenti, *"un comportamento socialmente dannoso ed il complesso sistema sanzionatorio del decreto sarebbe inteso a suggerire alla persona giuridica di attivarsi per un recupero della legalità della sua condotta tramite meccanismi di reintegrazione dell'offesa e di riorganizzazione aziendale"*[7].

La "responsabilità da reato"

In conclusione, si può dire, pacificamente, che la natura della responsabilità in esame introduca un nuovo diritto punitivo e sanzionatorio, non completamente penale ne tantomeno amministrativo, configurandosi in una sorta di *tertium genus*[8]. Il termine utilizzato, dunque, per racchiudere questa posizione, è stato quello di *"responsabilità da reato"* [9], che esprime con immediatezza il problema di disciplina cui la nuova normativa ha inteso dare risposta, evocando inoltre il contenuto precettivo e sanzionatorio di tali istituti.

[7] DOLCINI E., *Principi costituzionali e diritto penale alle soglie del terzo millennio. Riflessioni in tema di fonti, diritto penale minimo, responsabilità degli enti e sanzini,* in *Rivista italiana di diritto e procedura penale,* 1999, pag. 10.

[8] In questo senso, fra i tanti, PIERGALLINI C., *Sistema sanzionatorio e reati previsti dal codice penale,* in *Diritto penale e procedura,* 2001, pag. 1365; VINCIGUERRA S., *Quale specie di illecito,* in VINCIGUERRA-CERESA GASTALDO-ROSSI, *La responsabilità dell'ente per il reato commesso nel suo interesse,* Cedam, Padova, 2004, pag. 183.

[9] Termine coniato da PULITANO' P., *La responsabilità da "reato" degli enti: i criteri d'imputazione*, in *Rivista italiana di diritto e procedura penale,* 2002, pag. 420.

2. Lineamenti essenziali della responsabilità delle persone giuridiche da reato; i modelli organizzativi e la tipologia delle sanzioni

Giunti a questo punto, appare necessario fornire, quantomeno sinteticamente, i contenuti essenziali del decreto 231, analizzando i soggetti destinatari della disciplina, i criteri di imputazione, le sanzioni ed i modelli organizzativi, così da capirne la relazione con i reati privacy trattati nei capitoli addietro.

I soggetti: gli enti

Innanzitutto, quanto ai soggetti, il decreto è applicato agli enti[10] forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica. È poi detto che il decreto non si applica allo Stato, agli enti pubblici territoriali (quindi Regioni, Province e Comuni), agli enti pubblici non economici nonché agli enti che svolgono funzioni di rilievo costituzionale[11].

Gli apicali ed i sottoposti

Per quanto concerne la sussistenza della responsabilità da reato dell'ente, devono essere soddisfatti alcuni criteri di imputazione; l'illecito deve, infatti, essere stato commesso nell'interesse o vantaggio dell'ente e deve essere stato realizzato da soggetti che siano legati all'ente stesso da una particolare tipologia di rapporto. Tali persone sono coloro i quali rivestono funzioni di rappresentanza, amministrazione o direzione dell'ente o di una sua unità organizzativa dotata di una certa autonomia nonché persone che esercitano anche di fatto la gestione e i controllo dello stesso e coloro i quali sono sottoposti alla direzione o alla vigilanza di uno dei soggetti di cui *supra*[12].

La prima classe di soggetti è definita "apicali", mentre la seconda "sottoposti". Come accennato, ulteriore presupposto per rinvenirsi responsabilità è che, tali soggetti abbiano agito delittuosamente nell'interesse o vantaggio dell'ente;

[10] Dizione richiesta specificamente dalla Relazione al decreto, nella quale si disse di utilizzare il termine ente piuttosto che persona giuridica, per la ragione che quest'ultimo termine, essendo riferibile esclusivamente a soggetti aventi personalità giuridica, avrebbe dovuto *"essere dilatato troppo al di là della sua capacità semantica al fine di poter ricomprendere anche gli enti che tale requisito non hanno"*.

[11] Basti pensare ai partiti politici e ai sindacati.

[12] Il legislatore, nel disegnare i soggetti qui citati, si è rifatto, come si legge nella Relazione, alle indicazioni provenienti dal modello della cosiddetta "teoria organica" per cui l'identità fra autore dell'illecito e destinatario della sanzione viene assicurata quando la persona fisica autrice del reato è un soggetto che ha agito nell'interesse o a vantaggio dell'ente; in questo senso, quando si raggiunge la prova dell'esistenza di un collegamento rilevante fra individuo e persona giuridica, è ben possibile riconoscere nell'organizzazione una protagonista della vicenda criminosa.

quindi, per riconoscersi tale responsabilità non basterà che la persona fisica abbia agito per conto dell'ente, dovendosi altresì considerare anche le conseguenze che l'ente ha ottenuto o poteva ottenere dalla condotta delittuosa altrui.

Interesse e vantaggio

Per interesse, in giurisprudenza, si sono individuate le seguenti caratteristiche, ovvero la sua natura squisitamente soggettiva, da riferirsi alla sfera volitiva del soggetto che pone in essere la condotta, per cui l'interesse deve ritenersi suscettibile di una valutazione *ex ante*. Il vantaggio, invece, presenta caratteristiche oggettive, che saranno da valutare *ex post* e quindi alla luce di quelle che sono poi state le conseguenze del comportamento delittuoso del singolo[13].

Inoltre, in presenza di questi due requisiti, ovvero la commissione da parte di determinati soggetti di alcuni illeciti nell'interesse o vantaggio per l'ente, si richiede che vi sia *"pur sempre uno specifico legame fra il reato commesso ed il comportamento dell'ente"*[14], del quale poi bisogna accertare l'atteggiamento colpevole.

La colpa di organizzazione

Il legislatore ha individuato la fonte di tale colpevolezza in una sorta di "colpa di organizzazione", per cui l'ente dovrebbe rispondere del reato commesso da alcune persone fisiche solo di fronte ad eventuali lacune e manchevolezze nell'organizzazione della sua attività che abbiano consentito a quei soggetti di porre in essere condotte delittuose. Se il reato è commesso da un apicale, la disciplina prevede che l'onere della prova contraria spetti all'ente, di modo che l'ente stesso debba identificarsi con la persona che ha agito nel suo interesse o vantaggio con la conseguenza che in questa ipotesi di reato, vada considerato come fosse stato commesso proprio dalla persona giuridica.

---

[13] Riprendendo una celebre posizione della sentenza di Cassazione n. 3615 del 2005: "*in tema di responsabilità da reato delle persone giuridiche e delle società, l'espressione normativa con cui se ne individua il presupposto nella commissione dei reati nel suo interesse o a suo vantaggio, non contiene un'endiadi, perché i termini hanno riguardo a concetti giuridicamente diversi, potendosi distinguere un interesse a monte per effetto di un indebito arricchimento, prefigurato e magari non realizzato in conseguenza dell'illecito, da un vantaggio obbiettivamente conseguito con la commissione del reato, seppure non prospettato* ex ante*, sicché l'interesse e d il vantaggio sono in concorso reale*".

[14] DI GIOVINE O., *Lineamenti sostanziali del nuovo illecito punitivo,* in *Reati e responsabilità degli enti. Guida al D.lgs 8 giugno 2001 n. 231,* a cura di LATTANZI, Milano, 2005, pag. 79.

Essa sarà esente da responsabilità solo se dimostri che abbia assunto tutte le misure necessarie ad impedire la commissione di delitti del tipo di quello verificatosi, vale a dire: aver adottato e applicato efficaci controlli preventivi per impedire la commissione dei reati; aver istituito nell'ente, per garantire la massima efficienza dei modelli organizzativi, un apposito organo di controllo con piena autonomia e iniziativa nell'attività di supervisione; che i soggetti apicali hanno commesso il reato eludendo fraudolentemente i protocolli preventivi; che non si sono verificate omissioni o negligenze nell'operato dell'organo di controllo.

I modelli organizzativi

Si capisce, dunque, che, ad elemento centrale, assurge la figura dei modelli organizzativi[15] i quali, pur non essendo obbligatori, per via dei costi, sono essenziali al fine di evitare di rispondere del reato commesso da altri soggetti. Tali modelli, si intende, non debbono risultare come semplice documento formale ma, col supporto degli organi di gestione e controllo, dovranno essere concretamente attuati al fine di ridurre il rischio della commissioni dei reati del presente decreto.

Se il reato è invece commesso da un sottoposto, la disciplina muta, in quanto l'ente sarà responsabile solo ove la pubblica accusa dimostri che la commissione del reato è stata resa possibile dall'inosservanze degli obblighi di direzione o vigilanza che gravano sulla persona giuridica.

Infine, in ogni caso, è esclusa l'inosservanza degli obblighi in questione se l'ente, prima della commissione di un reato, ha adottato ed efficacemente attuato un modello di organizzazione idoneo, secondo una valutazione *ex ante* ed astratta, a prevenire i reati della specie di quello verificatosi.

[15] Mutuati dalla giurisprudenza americana: cd. "*compliance programms*". Tali modelli, ai sensi del decreto 231, devono prevedere quanto segue: individuare le attività nel cui ambito possono essere commessi i reati; predisporre specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire; individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati; prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e sull'osservanza del modello organizzativo; introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello organizzativo.

L'apparato sanzionatorio

Venendo, infine, alle sanzioni, all'ente sono applicabili la sanzione pecuniaria, tramite un sistema per quote[16], le sanzioni interdittive[17], la pubblicazione della sentenza e la confisca. Il sistema in questione è stato definito a "doppio binario"[18], poiché la natura delle sanzioni applicabili è duplice, in quanto possono essere pecuniarie o interdittive, tuttavia mentre le prime sono indefettibili e quindi saranno comminate ogni qualvolta vi sia una dichiarazione di responsabilità della società, le seconde troveranno applicazione solo in riferimento ad un novero selezionato di fatti concreti che abbiano raggiunto una certa soglia di elevata gravità, al fine di garantire il rispetto dei principi di adeguatezza o proporzionalità. Soprattutto per quanto riguarda le interdittive, la loro previsione è elemento caratterizzante del decreto 231 dal momento che tale posizione sopperisce all'incapacità della pena pecuniaria, se applicata isolatamente, di contrastare la criminalità di impresa. Per quanto concerne la pubblicazione della sentenza[19], sarà disposta dal giudice che, in mancanza di disposizioni normative, dovrà valutare *sua sponte* se essa possa risultare utile nell'ottica della repressione del fatto illecito e della prevenzione rispetto alla futura commissione di fatti illeciti simili. Circa la confisca, invece, essa è una sanzione autonoma ed obbligatoria, che è sempre disposta, con la sentenza di condanna, requisendo il prezzo o il profitto del reato, salvo che per la parte che può essere restituita al danneggiato, facendo ovviamente salvi i diritti acquisiti dai terzi in buona fede.

[16] È ricalcato il sistema dei cd. tassi giornalieri assai conosciuto nel panorama europeo, con il quale, moltiplicando la quota (da 100 a 1.000) di ogni reato commesso per alcuni elementi che tengono conto anche della capacità patrimoniale della società (affidato al giudice), si bilancia di volta in volta la sanzione con la potenza monetaria della società.

[17] Che sono l'interdizione dall'esercizio dell'attività; la sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; il divieto di contrattare con la pubblica amministrazione salvo che per ottenere le prestazioni di un pubblico servizio; l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi.

[18] DE VERO G., *Il sistema sanzionatorio di responsabilità ex crimine degli enti collettivi,* in *La responsabilità amministrativa delle società e degli enti,* 2006, 2, pag. 173.

[19] Che ricalca, invece, la *adverse publicity* dell'ordinamento americano.

3. L'introduzione da parte della L. 48/2008 nel D.lgs 231/2001 dell'art. 24 bis rubricato "Delitti informatici e trattamento illecito di dati"

L'introduzione dell'art. 24 bis

La già citata Legge n. 48 del 2008, dando attuazione alla Convenzione Cybercrime di Budapest del 2001, ha introdotto, inoltre, l'art. 24 bis[20] all'interno del D.lgs 231/2001, rubricato "Delitti informatici e trattamento illecito di dati"[21]. Tale norma dà attuazione all'art. 12 della Convenzione, che vincolava le parti a prevedere, con l'adozione di misure compatibili con i principi del proprio ordinamento giuridico, una forma di responsabilità per le persone giuridiche nell'interesse o a vantaggio delle quali fossero stati compiuti reati informatici. Ovviamente, come visto in sede di trattazione generale, permane, per gli enti, la possibilità di ridurre il rischio di violazione della legge penale predisponendo *"modelli organizzativi che individuino le sedi, le modalità e le finalità del compimento dei relativi reati, così da predisporre una rete di controlli atta a garantire la massima trasparenza alle operazioni informatiche, sia a livello apicale, sia fra i dipendenti"*[22].

Soprattutto in riferimento ai reati informatici, la necessità di modelli organizzativi adeguati è assai pressante; tali reati, infatti, lo si è visto, hanno

---

[20] Si riporta il contenuto completo dell'articolo ricordando, come si vedrà tra poco, che parte di esso è stato modificato e, successivamente rimodificato, introducendo e poi eliminando il riferimento al Codice della privacy:
1. In relazione alla commissione dei delitti di cui agli articoli 615-*ter*, 617-*qua*ter, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.
2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.
3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.
4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

[21] Infatti, si è rilevato come, nonostante la rubrica, mancasse il riferimento al trattamento illecito di dati ex. art. 167 del Codice Privacy: SARZANA C., IPPOLITO S., *La legge di ratifica della Convenzione id Budapest: una gatta legislativa frettolosa*, in *Diritto e procedura penale*, 2008, pag. 1562.

[22] BELLUTA H., *Cybercrime e responsabilità degli enti,* in AA.VV., *Sistema penale e criminalità informatica,* in LUPARIA L., Giuffrè, Milano, 2009, pag. 90.

come caratteristica che, ancor più nel contesto organizzato di una struttura aziendale, dove terminali e password possono circolare fra gruppi di dipendenti e dirigenti, risulterà assai difficile rintracciare una persona fisica alla quale attribuire il possibile compimento del reato. Saranno dunque richiesti adeguati modelli organizzativi, di gestione e controllo che garantiscano la trasparenza delle decisioni aziendali e dei flussi informatici di dati, tramite un criterio di tracciabilità delle decisioni e delle operazioni, per impedire o almeno facilmente rintracciare l'individuazione delle condotte di illecito utilizzo di tali strutture informatiche aziendali.

I reati privacy informatici introdotti nel decreto 231

Venendo ai reati richiamati nell'art. 24 bis, questi sono caratterizzati da tutte quelle condotte accomunate dall'essere dirette a danneggiare un sistema informatico: l'accesso abusivo ad un sistema informatico o telematico (615 ter), l'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (617 quater), l'installazione di apparecchiature predisposte a tal fine (617 quinquies), il danneggiamento di informazioni, dati e programmi informatici (635 bis), il danneggiamento di informazioni, dati e programmi utilizzati da Stato, ente pubblico o di altra utilità (635 ter), il danneggiamento di sistemi informatici o telematici (635 quater), il danneggiamento di analoghi sistemi di pubblica utilità (635 quinquies)[23].

Al 2° comma sono contemplate le due fattispecie di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (615 quater) e della diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies)[24].

[23] Per tutti questi reati è prevista la sanzione pecuniaria da 100 a 500 quote e le sanzioni interdittive previste dall'art. 9, coma 2, lettere a,b,e del d.lgs 231/2001.

[24] Esse sono figure delittuose accessorie rispetto a quelle indicate al comma 1° a mezzo delle wquali il danneggiamento si realizza nel momento in cui i codici o i programmi vengono utilizzati per porre in essere accessi abusivi, intercettazioni, impedimenti o interruzioni di comunicazioni informatiche o telematiche. Per questi reati è prevista la sanzione pecuniaria sino a 300 quote e le sanzioni interdittive delle lettere b ed e di cui *supra*.

L'ultimo comma tratta invece i reati di falso in documento informatico (art. 490) e frode informatica del soggetto che presta servizi di certificazione di firma elettronica (640 quinquies)[25].

Subito appare evidente, tuttavia, la mancata previsione della responsabilità giuridica egli enti in dipendenza del reato di frode informatica "semplice" (640 ter), di indubbia rilevanza nel novero dei reati informatici. Alcuni hanno motivato questa omissione, dicendo che possa trattarsi di "*sviste inconsapevoli*"[26] in virtù del silenzio dei lavori preparatori, che provocano una certa disparità di trattamento del tutto irragionevole, in quanto a ciò non sarà nemmeno possibile rimediare in sede interpretativa fintanto che vale il principio di legalità dell'illecito amministrativo di cui all'art. 1 L. 689/1981 espressamente ribadita dall'art. 2 del decreto 231, che non consente l'ampliamento dell'ambito delineato dagli artt. 24 e 24 bis *in malam partem*, fino a ricomprendervi fattispecie non indicate dal legislatore.

Casi pratici nella rete aziendale

Rimandando all'analisi degli articoli specifici per la loro comprensione, si vuole, ora, fornire alcuni risvolti pratici, raggruppando i reati per genere, che sottolineino i rischi derivanti per i beni giuridici tutelati da tali reati fra i quali, si ricorda, la riservatezza.

Il primo caso potrebbe essere quello di un accesso abusivo compiuto da un dipendente, rivolto verso un sistema, esterno o anche interno all'azienda, interconnesso a una rete (come Internet o Intranet), per cui non si possiede nessun tipo di autorizzazione. In questi casi, solitamente, si tratta di attacchi sferzati tramite connessioni triangolate su server esteri, così che la ricostruzione del percorso effettuato per raggiungere il sistema risulti altamente complessa[27]. Inoltre, soprattutto per quanto concerne il contenuto

[25] Sono questi reati il cui tratto comune consiste di essere fattispecie che si compiono attraverso l'uso di sistemi informatici e non su di essi, come per gli altri due commi. Sono puniti con la sanzione pecuniaria fino a 400 quote e la sanzione interdittiva delle lettere c, d, e.

[26] Così DEZZANI G., *La responsabilità amministrativa degli enti collettivi,* in AA.VV., in *Reati informatici,* Cedam, Milano, 2010, pag. 238.

[27] Dovrebbero, in tal caso, richiedersi infatti diverse rogatorie internazionali. "*Basti pensare al fatto che è possibile compiere un accesso ad un computer collegato alla rete nella stessa città costruendo un percorso digitale che coinvolge host in tutti i continenti*": DEZZANI G., *Una nuova ipotesi di*

del modello organizzativo, c'è da rilevare il caso dell'hacker che, solitamente, attacca il sistema in questione soltanto con lo scopo di dimostrare le sue eccelse capacità informatiche. In questo caso i danni sarebbero solamente riferibili ai sistemi informatici ed ai sistema di sicurezza, eppure, si è ritenuto che anche un caso del genere debba essere disciplinato all'interno dei modelli organizzativi e nei sistemi di controllo dell'organismo di vigilanza, in quanto, altrimenti, gli apicali potrebbero tendere a oscurare eventi di questo tipo, pur di non rendere migliorabile il proprio sistema, riducendo in questo modo i costi. Da questa eventualità, però, si distingue quella posta in essere dal cd. "*cracker",* ovvero colui che, non semplicemente dimostra la propria bravura, ma ha anche come intento quello di danneggiare o eliminare irreversibilmente i dati del sistema. Questo caso, assai più grave, deve essere, come il primo, oggetto analitico del modello organizzativo e dell'organismo di vigilanza.

Esiste poi una ulteriore tipologia di accesso abusivo, ovvero quella nel quale si dispone delle credenziali per accedere, ma per una funzione differente da quella in cui viene l'accesso[28]. Questo è, probabilmente, il più frequente illecito che può avvenire all'interno di una struttura di rete aziendale, infatti manca il confronto con l'hacker o cracker e, invece, spesso si tratta di dipendenti infedeli o utenti di sistema curiosi che tentano di accedere ad una certa area dell'azienda senza esserne autorizzati. Ciò può ben avvenire cercando di acquisire l'identità di un collega carpendone le credenziali, nome utente e password, e dunque, l'espressione di volontà da parte di chi ha il diritto di escluderlo sarà espressa dall'amministratore di sistema con la configurazione dei diritti di accesso al cui tentativo di forzatura recepisce un errore di accesso negato.

Venendo ad esempi di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, un frequente attacco è il cd.

---

reato degli enti collettivi: la criminalità informatica, in *La responsabilità amministrativa delle societa e degli enti,* 2010, pag 71.

[28] Come prelevare dati da una cartella er cui on si ha autorizzazione all'interno di un determinato server.

"Denial of Service", detto anche DoS, col quale si intende negazione del servizio. Esso si configura quando, ad esempio l'hacker, attaccando un server, modifichi la pagina iniziale del servizio con una a suo piacere, per lasciare una traccia del suo passaggio[29].

Inoltre, i casi come quelli appena visti, possono anche essere compiuti nel perimetro di una rete informatica aziendale propria, tramite un comportamento scorretto dell'utente, quindi nei confronti dei propri server. Ciò può accadere se un utente installi illecitamente un software e lo impieghi per trasmissioni di dati che non rientrano nello scopo per ci gli è stato assegnato un certo sistema informatico, potendo così eventualmente dar vita al reato ex. art. 617 cp.

La struttura del modello organizzativo

Venendo ora alla composizione di un modello organizzativo adeguato a ridurre i rischi dei reati di cui sopra, solitamente si introducono due differenti documenti[30]. Il primo, indispensabile, è un progetto di sicurezza, denominato *Target of Evaluation* (ToE), il quale indica la valutazione di ciò che deve essere protetto, cioè i sistemi informatici e telematici, di quanto è il loro valore economico e di quanto è necessario spendere per la loro protezione. Come è ovvio, non esiste uno standard, in quanto ogni azienda effettua un uso dell'informatica fortemente personalizzato ed il valore dei propri dati è tarato conseguentemente sulle proprie risorse. Tale progetto, al suo interno, conterrà la prevenzione di tutte le fattispecie di reato che abbiano origine dall'esterno della rete aziendale e, inoltre, tutti i possibili reati che possono essere compiuti dagli utenti interni della rete aziendale. Per quanto riguarda il secondo documento, esso si integrerà con il Codice Etico[31] ed il Documento di Politica Aziendale[32], prevedendo un capitolo studiato appositamente per disciplinare

[29] Tra l'altro, si ritiene la configurabilità di un DoS, anche di fronte ad una inusuale lentezza della rete informatica o telematica. Infatti la legislazione prevede non solo la interruzione ma anche l'impedimento di servizio, dunque anche se il DoS non comporta l'interruzione totale del sistema, ma provoca anche solo un rallentamento, può comunque considerarsi commesso il reato.

[30] DEZZANI G., *cit.*, pag. 78.

[31] È quel documento sempre presente in un modello organizzativo 231 che prevede buone regole di trasparenza, correttezza e responsabilità per i dipendenti e gli apicali dell'azienda, contenendo inoltre i principi fondamentali, diritti e doveri inerenti ai comportamenti e alla responsabilità della società.

[32] Che è, invece, un documento, come dice il nome, che organizza e amministra gli interessi primari nella società, ai quali mira per il proprio soddisfacimento economico.

l'uso del sistema informatico all'interno dell'azienda. Saranno quindi esplicitati i sistemi di controllo messi in opera al fine di monitorare l'attività dei dipendenti, dichiarando anche i limiti di impiego della struttura (come nell'uso di internet e di posta elettronica). In questa sezione saranno, di conseguenza, approfonditi aspetti quali il documentare ed impedire comportamenti illeciti come l'uso di password non autorizzate, detenzione o installazione di software non esplicitamente previsti dall'azienda, escludere la ovvia detenzione di virus, spyware di ogni genere e dispositivi atti all'interruzione di servizi o alle intercettazioni, tali da commettere illeciti nel perimetro aziendale. Si aggiunga, a ciò, che in tale ottica sarà di assoluta importanza la nomina di un amministratore di sistema e di un responsabile delle credenziali di accesso, anche nel rispetto della parte civilistica del Codice della Privacy, di cui si è accennato nel corso di questo elaborato.

Tale figura avrà un ruolo centrale, come nel caso dell'attività d'analisi dei *competitors*[33]; essi infatti potrebbero sempre agire per procurarsi abusivamente i codici di accesso ed introdursi nel sistema di questi ultimi anche se protetto da misure di sicurezza per poi permanervi contro la volontà espressa o tacita di chi ha il diritto di escluderlo, per conseguire un vantaggio ingiusto per la propria azienda, anche a danno della riservatezza dei dipendenti dell'altra[34].

Per questo motivo, istituire una tale figura di responsabile appare la soluzione migliore, in quanto tutte le attività di gestione delle procedure informatiche, come il controllo degli accessi e della sicurezza, dovrebbero essere demandate a questa figura professionale con l'impiego di sistemi automatici [35] di monitoraggio che permettano di presidiare continuativamente tutte le attività

[33] Ovvero i principali antagonisti sul mercato di particolari enti di rilevante importanza economico-produttiva.

[34] Si veda, in questo senso, DEZZANI G., PICCINNI L. M., *Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito dei applicazione del d.lgs. 231/2001,* in *La responsabilità amministrativa delle società e degli enti,* 2011, pag. 43.

[35] Sempre più diffusa è l'adozione di sistemi di *audit* automatico della struttura informatica, cioè software progettati per tenere traccia di tutte le attività che avvengono sulla rete e permettono di ricostruire con gran facilità la movimentazione e l'alterazione di un dato nel sistema. Questi software garantiscono l'assoluto anonimato dell'utente incrociando le informazioni con i files di log, ed è possibile risalire all'uso di una risorsa e determinare cosi la commissione di un reato.

svolte dagli utenti e generare eventuali segnali di allerta via email o sms all'amministratore del sistema.

Infine, si evidenzia che con la Legge n. 35 del 2012, non è più richiesto, per le aziende rientranti nel decreto 231, il possesso del Documento Programmatico sulla Sicurezza del 2006, con il quale si obbligavano gli enti a predisporre ed aggiornare annualmente entro tale documento, per attestare la corretta adozione delle previste procedure che riguardano il trattamento dei dati personali e soddisfare anche determinati obblighi di legge[36]. Tale rimozione fu certamente dovuta alla necessità del Governo di tagliare i costi che gravano su determinate aziende come conseguenza della crisi finanziaria attuale. In ogni caso, permane comunque l'obbligo, per l'azienda, di inserire un documento esplicativo di tutti i termini tecnici necessari per l'utente al fine di evitare il compimento dei reati di cui *supra*.

A conclusione c'è da dire che, nonostante il settore informatico sia entrato a far parte del panorama dei reati per cui si deve prevedere uno spazio nel modello organizzativo, i procedimenti che hanno come oggetto reati di questo tipo sono estremamente limitati poiché, principalmente, nella maggior parte dei casi essi non vengono denunciati[37]. La denuncia è infatti vista come un'ammissione di vulnerabilità del proprio sistema informatico, con successive conseguenze anche sul piano della credibilità dell'azienda nei confronti dei consumatori, come nel caso delle banche.

---

[36] Tra i quali si rammentano, l'elenco dei trattamenti di dati personali; la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati; l'analisi dei rischi che incombono sui dati;le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità; a descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23; la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

[37] In linea con questa posizione è anche DEZZANI G., *Una nuova ipotesi di reato degli enti collettivi: la criminalità informatica,* in *La responsabilità amministrativa delle società e degli enti,* 2010, pag 80.

4. Il D.L. 93/2013 e l'aggiunta dei reati privacy all'interno dell'art. 24 bis del D.lgs 231/2001; la loro mancata conversione con la L. 113/2013; de iure condendo: il Regolamento Europeo sui dati personali

I reati privacy propri del decreto 231: D.L. 93/2013

Nel corso dell'estate 2013 è stato varato il D.L. 93/2013 che, fra le altre cose[38], ha apportato una significativa modifica all'art. 24 bis del decreto 231. Di fatti, il comma 1° è stato modificato come segue: *"in relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quarter, 635-quinquies e 640-ter, terzo comma, del codice penale nonché dei delitti di cui agli articoli 55, comma 9, del decreto legislativo 21 novembre 2007, n. 231[39], e di cui alla Parte III, Titolo III, Capo II del decreto legislativo 30 giugno 2003, n. 196, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote"*.

Come si vede, il riferimento all'intera gamma di reati posti a tutela della privacy propri del Codice del trattamento dei dati personali è evidente, come anche il riferimento all'art. 640 ter comma 3°, in tema di furto di identità digitale. Ciò che ha spinto il legislatore all'introduzione di questi reati è sintetizzabile come segue: innanzitutto, la Convenzione di Budapest del 2001, così come aveva imposto agli Stati Membri la produzione di una normativa tale da coprire penalmente l'eventualità del compimento di *computer crimes* in tema aziendale, allo stesso modo aveva previsto l'introduzione di una tutela simile anche per quanto riguardasse il trattamento illecito dei dati personali che, lo si è visto, in Italia è disciplinato dal D.lgs 196/2003. Eppure, come si è analizzato nel corso del paragrafo precedente, la L. 48/2008 che traduce nel panorama italiano la normativa proveniente dalla Convenzione del 2001, ha mancato di introdurre, nel novero dell'art. 24 bis del decreto 231, tali reati

[38] Tale decreto aveva il seguente nome: "Disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province". Oltre alla modifica sul decreto 231 esso proponeva riforme in tema di maltrattamenti in famiglia, violenza sessuale ed atti persecutori, rapina, furto e frode informatica, ulteriori modifiche al codice di procedura penale. Si ricorda, per'altro, che la modifica in tema di frode informatica è quella, già analizzata *supra*, circa il furto di identità digitale.

[39] Che sanziona la condotta di abusivo utilizzo di altrui carte di crediti e mezzi elettronici di pagamento.

privacy propri. Inoltre, proprio la modifica apportata dalla legge del 2008 prevede, nella rubrica dell'art. 24 bis, anche il riferimento al trattamento illecito dei dati che, però, non è contemplato nel contenuto del medesimo articolo. Per queste ragioni, la soluzione del Governo è sicuramente apprezzabile e coerente con il panorama europeo in tema di *computer crimes*. Si aggiunga, tra le altre cose, che tale modifica è stata ritenuta, dalla Cassazione[40], *"di grande impatto, soprattutto per la configurazione della responsabilità da reato degli enti per l'illecito trattamento dei dati, violazione potenzialmente in grado di interessare l'intera platea delle società commerciali e delle associazioni private soggette alle disposizioni del d.lgs 231/2001"*.

Le critiche dottrinarie a tale introduzione

Eppure, certa dottrina ha immediatamente criticato l'intervento in questione, nel periodo in cui esso doveva ancora essere oggetto di conversione da parte del Parlamento. Si è infatti ritenuto che, nonostante si trattasse di una previsione di per sé apprezzabile, essendo condivisibile l'estensione della responsabilità delle persone giuridiche a tali ulteriori fattispecie, fosse tuttavia inserita nell'ambito di una disposizione secondo modalità e per ragioni di difficile comprensione, "*considerato che, ad esempio, non si comprende quali siano i rapporti correnti fra il reato di illecito utilizzo di carte di credito ed i delitti in materia informatica"*[41]. Tuttavia, lo si vuole ribadire, l'introduzione di questi reati è da ritenersi soddisfacente, quantomeno considerando sistematicamente il tema dei *computer crimes*, poiché, in questo modo, esso è perfettamente sovrapponibile alle proposizioni di stampo europeo cominciato con la Convenzione di Budapest del 2001. La loro introduzione consentirebbe di chiudere il cerchio in tema di riservatezza informatica, tutelando in maniera definitiva la privacy di coloro i quali posseggono elevati dati sensibili trattati nel panorama aziendale, in quanto gli articoli sopra evidenziati, già introdotti con la legge del 48, affrontano il problema solo trasversalmente e mai di petto,

[40] PISTORELLI L., *Relazione di Cassazione n. III/01/2013,* 28 agosto 2013, pag. 7.
[41] Così SANTORIELLO C., *Un osservazione sul Decreto Legge 93/2013,* in *Rivista 231,* 2013, consultato in Agosto 2014, http://www.rivista231.it/Legge231/Pagina.asp?Id=933.

come farebbe invece l'introduzione delle sanzioni penali proprie del Codice della Privacy.

Il vero problema, in realtà, risiede nel fatto che la loro introduzione è figlia non di una legge del Parlamento, bensì di un Decreto Legge, di provenienza governativa, con i conseguenti dubbi già proposti addietro relativamente ai principi base del diritto penale.

La mancata conversione nella L. 113/2013 delle modifiche dell'art. 24 bis

Non è un caso, infatti, che poco dopo, nell'ottobre 2013, la legge di conversione n. 113 non ha confermato il contenuto di cui *supra* del D.L. 93/2013. Tra l'altro, per le stesse ragioni sopra esposte, medesima dottrina ha commentato positivamente tale mancata conversione[42].

In primis, c'è da rilevare che, quantomeno sul piano della successione delle leggi penali del tempo, tale mancata conversione, per quanto inevitabile, non è stata una mossa convincente. Difatti, sebbene non sembrano esser pervenuti, nelle aule di giustizia, casi di applicazione dell'art. 24 bis modificato dal D.L 93/2013 nei 60 giorni successivi alla sua produzione, sicuramente vi sarebbero stati elevati problemi di applicazione di tale normativa, considerando la disposizioni previste dal Codice Penale all'art. 2 e le irrisolte problematiche circa la responsabilità penale o amministrativa derivante dalle disposizioni del decreto 231[43].

Inoltre, bisogna dire che, a ragione della mancata conversione, il Parlamento si è trovato di fronte anche ad evidenti motivazioni politiche. Non può negarsi, soprattutto in un periodo delicato come quello attuale, che l'attuazione di ulteriori modelli atti a ridurre il rischio del compimento dei reati di cui al Codice Privacy, avrebbe richiesto un esborso economico non indifferente, e soprattutto assai elevato per tutte quelle società che fanno della mobilità dei dati, anche sensibili, uno dei loro punti di forza.

---

[42] SANTORIELLO C., *Una ulteriore osservazione sul Decreto Legge 93/2013,* in *Rivista 231,* 2013, consultato in Agosto 2014, http://www.rivista231.it/Legge231/Pagina.asp?Id=942.

[43] Tra l'altro, il problema sarebbe stato più complesso di quanto potrebbe apparire, in quanto non ci si troverebbe di fronte all'applicazione della legge penale più favorevole, considerando che l'art. 24 bis, nella parte in cui avrebbe previsto una responsabilità per i reati privacy propri, non è un vero e proprio "reato", tenuto conto delle considerazioni in tema di responsabilità amministrativa da reato, oscillanti fra il penale, il civile e l'amministrativo.

A ciò si aggiunga, anche per i medesimi motivi economici, la non indifferente spinta contraria alla conversione rilevata dal Presidente di Confindustria Giorgio Squinzi, il quale chiedeva l'abrogazione del relativo articolo, tornando ad escludere la Privacy dai reati previsti dal decreto 231.

Conseguentemente, il testo definitivo promulgato dalla L. 113/2013 dell'art. 24 bis, comma 1°, risulta così configurato: "*in relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote*". Dunque, al momento, i reati privacy propri non sono previsti all'interno del novero dei reati punibili nei confronti delle persone giuridiche secondo il D.lgs 231/2001 mentre, come si è visto, i reati privacy impropri, escluso l'art. 640 ter, sono tutti ampiamente presenti nel decreto.

De iure condendo: il Regolamento Europeo

A conclusione del nostro discorso, rimane, infine, da fare un riferimento circa il futuro Regolamento Europeo sulla protezione dei dati personali il quale andrà a sostituire completamente la vecchia direttiva 95/46/CE in tema di privacy. Al giorno d'oggi tale regolamento è ancora in fase embrionale, in quanto è stato oggetto solo di una prima lettura da parte del Parlamento Europeo[44] e, dunque, probabilmente, sarà futuro oggetto di ulteriori modifiche. Prima di tutto è il caso di ricordare che il regolamento, diversamente dalla direttiva, è un atto giuridico vincolante, diretto non solo agli stati membri, ma anche ai singoli; è un atto cd. *self-executing* ed è direttamente applicabile, nel senso che, a differenza delle direttive, non necessita di alcun atto di recepimento o di attuazione. Detto ciò, il regolamento in questione apporterà modifiche consistenti sul tema della riservatezza, soprattutto per quanto concerne proprio il rapporto con le persone giuridiche, amalgamandosi alla perfezione col decreto 231.

[44] Il 12 marzo 2014, il parlamento europeo ha votato tale nuovo regolamento europeo sulla protezione dei dati, la cui approvazione definitiva è attesa entro quest'anno, in coincidenza,tra l'altro, del semestre di presidenza italiana dell'Unione Europea: in prima lettura il regolamento è passato con 621 voti favorevoli e solo 10 contrari.

Il privacy officer

La figura più interessante per questo nostro tema, sulla quale è necessario porre in essere alcune considerazioni, è quella del cd. *privacy officer*[45] o *data protection officer*. Con esso si intende un soggetto la cui responsabilità è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali, e dunque la loro protezione, all'interno di un'azienda o di un ente, affinché questi siano trattatati in modo lecito e pertinente, nel rispetto delle normative.

Stando a quanto è desumibile dal contenuto dell'embrionale Regolamento, il *privacy officer* dovrà possedere conoscenza della normativa sulla gestione dei dati personali nel paese in cui opera, e dovrà inoltre garantire una sua consulenza per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, possedendo dunque conoscenza dei sistemi di gestione aziendali, per curare l'adozione di misure minime di sicurezza finalizzate alla tutela dei dati, che soddisfino i requisiti di legge e assicurino sicurezza e riservatezza. Poi, come è ovvio, in ragione del fatto che l'acquisizione e la gestione dei dati personali avviene in modo preponderante per mezzo digitale, il *privacy officer* deve altresì possedere competenze di carattere informatico.

Inoltre, sempre secondo la proposta di regolamento europeo sulla protezione dei dati personali, il responsabile del trattamento dei dati (nel caso italiano, il Garante) deve assicurarsi che *il privacy officer* sia prontamente coinvolto nelle questioni riguardanti la protezione dei dati personali, che adempia alle funzioni in piena indipendenza e non riceva istruzioni per quanto riguarda il loro esercizio, per questo, il *privacy officer* riferisce direttamente ai superiori.

[45] Anche se, da un punto di vista prettamente storico, la prima comparsa del privacy officer negli ordinamenti giuridici è stata in Europa, nella legislazione della Germania nel 1970 (*Datenschutzbeauftragter*), rimanendo tuttavia un caso isolato. La figura del privacy officer fu poi istituita per la prima volta negli USA nell'agosto 1999 dalla società AllAdvantage, specializzata in servizi pubblicitari via Internet. La figura fu creata per rispondere alla preoccupazione dei consumatori sull'utilizzo dei propri dati personali e per meglio gestire il rispetto delle norme legali inerenti al tema. Nel maggio del 2013, la posizione del privacy officer è stata introdotta nel personale presidenziale della Casa Bianca, negli Stati Uniti. L'amministrazione del Presidente Obama ha conferito tale incarico a Nicole Wong, che aveva diretto fino al novembre 2012 l'ufficio legale di Twitter, dopo essere stata in precedenza impiegata per otto anni negli uffici legali di Google.

Nel dettaglio, l'art. 37 del Regolamento[46] prevede, fra i più importanti, i seguenti compiti per tale soggetto: informare e consigliare il responsabile del trattamento in merito agli obblighi derivanti dal regolamento europeo e conservare la documentazione relativa a tale attività e alle risposte ricevute; sorvegliare l'attuazione e l'applicazione delle politiche del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità e la formazione del personale che partecipa ai trattamenti; sorvegliare l'attuazione e l'applicazione del regolamento europeo; garantire la conservazione della documentazione; controllare che le violazioni dei dati personali siano documentate, notificate e comunicate; controllare che il responsabile del trattamento effettui la valutazione d'impatto sulla protezione dei dati e richieda l'autorizzazione preventiva o la consultazione preventiva nei casi previsti; controllare che sia dato seguito alle richieste dell'autorità di controllo e, nell'ambito delle sue competenze, cooperare con l'autorità di controllo di propria iniziativa o su sua richiesta; fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento e, se del caso, consultare l'autorità di controllo di propria iniziativa.

Come è possibile vedere, l'introduzione futura del *privacy officer* deve considerarsi di grande impatto non solo per il tema della riservatezza in generale, ma soprattutto per risolvere anche il problema dell'inserimento dei reati privacy propri nel novero del decreto 231. Infatti, di fronte alla necessità di attuazione di tale figura, gran parte delle problematicità relative alla costituzione dei modelli organizzativi potrebbe venire meno, in quanto il *privacy officer* ben potrebbe risolvere tale criticità, sostituendo almeno in parte le previsioni richieste in un modello organizzativo per tali reati.

[46] Il testo del Regolamento Europeo, accompagnato da un interessante incipit esplicativo, è consultabile, per intero, in Italiano su: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_it.pdf

BIBLIOGRAFIA

ALBAMONTE E., *La responsabilità penale dell'internet provider: tra libertà di comunicazione e tutela dei singoli*, in *Questione giustizia*, 2010, 3, 184

ALESSANDRI A., *Reati d'impresa e modelli sanzionatori,* Giuffrè, Milano, 1984

ALESSANDRI A., *Riflessioni penalistiche sulla nuova disciplina,* in AA.VV., *Responsabilità d'impresa e strumenti internazionali anticorruzione,* a cura di SACERDOTI, Giuffrè, Milano, 2003

ALMA M., PERRONI C., *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Diritto penale e processo*, 1997, 505

AMATO G., *Contrasto specifico all'uso di dispositivi*, in *Guida al diritto,* 2008, 16, 58

AMATO G., *Danneggiamento perseguibile a querela*, in *Guida al diritto*, 2008, 16, 61

AMATO G., DESTITO V. S., DEZZANI G., SANTORIELLO C., *I reati informatici,* CEDAM, Padova, 2010

ANGIONI F., *Contenuto e funzioni del concetto di bene giuridico,* Giuffrè, Milano, 1983

ANTOLISEI F., *Manuale di Diritto Penale – Parte generale,* Milano, Giuffrè Editore, 2003

ANTOLISEI F., *Manuale di Diritto Penale – Parte speciale I,* Milano, Giuffrè Editore, 2003

ANTOLISEI F., *Il problema del bene giuridico,* in *Rivista italiana di diritto penale,* 1939, 3, 120

ANTONINI E., *Il trattamento illecito di dati personali nel codice della privacy: i nuovi confini della tutela penale,* in *Diritto penale e processo,* 2005, 3, 338

ARISTOTELE, *La politica,* Le Monnier, Firenze, 1981

ATERNO S., *Aspetti problematici dell'art. 615 quater c.p.,* in *Cassazione Penale,* 2000, 2, 389

BALDASSARRE A., *I diritti fondamentali nello Stato costituzionale*, in *Scritti in onere da Alberto Predieri* Tomo I, Milano 1996

BANI E., FERIOLI E. A., *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della Privacy"),* a cura di Bianca C. M, Busnelli F. D., Padova, CEDAM, 2007

BEDUSCHI L., *Caso Google: libertà d'espressione in Internet e tutela penale dell'onore e della riservatezza,* in *Corr. Merito,* 2010, 10, 963

BELLUTA H., *Cybercrime e responsabilità degli enti,* in AA.VV., *Sistema penale e criminalità informatica,* in LUPARIA L., Giuffrè, Milano, 2009

BELVEDERE A., *Riservatezza e strumenti d'informazione,* in *Dizionario del dir. priv.*, Milano, 1980, 1, 727

BERGHELLA R., BLAIOTTA P., *Diritto penale dell'informatica e beni giuridici*, in *Cassazione Penale*, 1995, 7, 1463

BLOUSTEIN E., *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, in *New York University Law Review*, 196439: pag. 962

BOISTEL A., *Cours de philosophie du dreoit,* Parigi, 1899

BORRELLI G., *Riprese filmate nel bagno di un pubblico esercizio garanzie costituzionali*, in *Cassazione Penale*, 2001, 12, 2453

BORRUSO R., *La tutela del documento e dei dati, in Profili penali dell'informatica,* Milano, 1994

BRANDEIS L.D., WARREN S., *The Right to Privacy,* in 4 Harward Law Review, 1890, p. 193

BRICOLA F., *Prospettive e limiti della tutela penale della riservatezza,* in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Milano, Giuffrè, 1970

BUSNELLI F. D., *Dalla legge al codice: un dilemma, una sfida, un consolidamento normativa, una (imperfetta) razionalizzazione delle tutele,* in *La protezione dei dati personali,* a cura di BIANCA C. M., BUSNELLI F. D., CEDAM, 2007, Padova, cap. XXXV

BUTTARELLI G., *Banche dati e tutela della riservatezza,* Milano, 1995

BUONOMO G., *Metodologia e disciplina delle indagini informatiche*, in BORRUSO-BUONOMO-CORASANITI-D'AIETTI, in *Profili penali dell'informatica*, Giuffrè, Milano, 1994

CAJANI F.,*La tutela penale dell'identità digitale alla luce delle novità introdotte dal D.L. 14 agosto 2013, n .93 (convertito con modificazioni dalla L. 15 ottobre 2013, n.119),* in *Cassazione Penale, 3*, 2014, 3, 109

CAJANI F., *Profili penali del phishing,* in *Cassazione Penale,* 2007, 13, 2299

CAJANI F., *La tutela penale dell'identità digitale alla luce delle novità introdotte dal D.L. 14 agosto 2013, n .93 (convertito con modificazioni dalla L. 15 ottobre 2013, n.119),* in *Cassazione Penale,* 2014, 3, 1103

CASSANO G., *Riflessioni a margine di un convegno sul caso Google/Vivi Down,* in *Riv. Pen.,* 2010, 10, 1026

CATAUDELLA A., *La tutela civile della vita privata*, Milano, Giuffrè, 1972

CECCACCI G., *Computer Crimes. La nuova disciplina dei reati informatici*, Giuffrè, Milano, 1994

CERRI A., voce *Riservatezza(diritto alla),* III parte – Diritto Costituzionale, in *Enciclopedia Giuridica Treccani*, Roma, 1999

CLANCY THOMAS K., *What does the Fourth Amendament Protect? Proprety, Privacy or Security?,* in *Wake Forest Law Review,* vol. 33, 1998, p. 344

CIRILLO G. P., *Il codice sulla protezione dei dati personali,* Milano, 2004,

COCCO P., *Beni giuridici funzionali* versus *bene giuridico personalistico,* in *Studi in onore di Giorgio Marinucci,* a cura di Dolcini e Paliero, Milano, 2006

COCCO P., *sub art. 615 quinquies*, in COCCO, AMBROSETTI, *Diritto Penale – Parte Speciale*, Cedam, 2013

COCCO G., *L'illecito degli enti dipendenti da reato ed il ruolo dei modelli di prevenzione,* in *Rivista italiana di diritto e procedura penale*, 2004, 1, 116

COOLEY T.C., *A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract,* Callaghan & Company, Chicago, IL, 1888

CORASANITI G., *Sanzioni penali e depenalizzazione degli illeciti nella normativa a tutela dei dati personali,* in *Danno e responsabilità,* 2002, 7, 698

CORDERO F., *Procedura Penale,* Giuffrè, Milano, 2003

CRESPI A., *La tutela penale del segreto*, Palermo, 1952

CUOMO-IZZI, *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico*, in *Cassazione Penale*, 2002, 7, 1021

D'AIETTI G., *Profili penali dell'informatica*, Giuffrè, Milano, 1994

D'AIETTI G., *La tutela dei programmi e dei sistemi informatici*, in BORRUSO, BUONUOMO, CORASANITI, D'AIETTI, *Profili penali dell'informatica*, Milano, 1994

DEL CORSO S., *La protezione dei dati personali,* a cura di BIANCA C. M., BUSNELLI F. D., CEDAM, Padova, 2007

DE CUPIS A., *I diritti della personalità,* in *Tratt. Di diritto civile e commerciale*, Giuffrè editore, Milano, 1982

DE FRANCESCO G.A., Lex specialis. *Specialità ed interferenza nel concorso di norme penali,* Milano, 1980

DELITALA, *Reati di pericolo,* in *Studi in onore di B. Petrocelli,* v. III, Milano 1972

DE PONTI P., *sub art. 615quinquies*, in MARINUCCI-DOLCINI, *Codice penale commentat*o, IPSOA, Milano, 2011

DESTITO V., DEZZANI G., SANTORIELLO C., *Il diritto penale delle nuove tecnologie*, Padova, 2007

DE VERO G., *Il sistema sanzionatorio di responsabilità ex crimine degli enti collettivi,* in *La responsabilità amministrativa delle società e degli enti,* 2006

DEZZANI G., *La responsabilità amministrativa degli enti collettivi,* in AA.VV., in *Reati informatici,* Cedam, Milano, 2010

DEZZANI G., *Una nuova ipotesi di reato degli enti collettivi: la criminalità informatica,* in *La responsabilità amministrativa delle società e degli enti,* 2010, 71

DEZZANI G., PICCINNI L. M., *Gli strumenti di sorveglianza aziendali per la prevenzione dei crimini informatici quali reati presupposto nell'ambito dei applicazione del d.lgs. 231/2001,* in *La responsabilità amministrativa delle società e degli enti,* 2011, 43

DEZZANI G., *Una nuova ipotesi di reato degli enti collettivi: la criminalità informatica,* in *La responsabilità amministrativa delle società e degli enti,* 2010, 80

DI GIOVINE O., *Lineamenti sostanziali del nuovo illecito punitivo,* in *Reati e responsabilità degli enti. Guida al D.lgs 8 giugno 2001 n. 231,* a cura di LATTANZI, Milano, 2005

DOLCINI E., *Principi costituzionali e diritto penale alle soglie del terzo millennio. Riflessioni in tema di fonti, diritto penale minimo, responsabilità degli enti e sanzioni,* in *Rivista italiana di diritto e procedura penale,* 1999, 1, 10

FERRI E., *Sociologia criminale*, 5* ed., vol. II, 1930

FIANDACA G., *Nessun reato senza offesa*, in FIANDACA G., DI CHIARA G., *Una introduzione al sistema penale. Per una lettura costituzionalmente orientata*, Jovene, Napoli, 2003

FIANDACA G., MUSCO E., *Diritto penale Parte speciale II,* Zanichelli, Bologna, 2012

FIANDACA G., MUSCO E.*, Perdita di legittimazione del diritto penale?*, in *Riv. it. dir. proc. pen*., 1994, 1, 23

FIORE S., *Riservatezza (diritto alla)*, Parte IV – Diritto Penale, in *Enciclopedia Giuridica Treccani,* Roma, 1998

FIORELLA, *Reato* (Voce), in *Enc. Dir.,* vol. XXXVIII, Milano, 1987

FLOR R., a nota di *Dir. Pen. e Processo*, 2005, 1, 81

FLORA G., *Il furto di identità,* in AA.VV., *Sicurezza e privacy: dalla carta ai bit*, a cura di COSTABILE, Esperta Edizioni, 2005

FOGLIA MANZILLO V., *Verso la configurazione della responsabilità penale per la persona giuridica,* in *Diritto e procedura penale,* 2000, 1, 196

FOIS S., *Questioni sul fondamento costituzionale del diritto alla «identità personale»* , in AA. VV., *L'informazione e i diritti della persona*, Jovene, Napoli, 1983

FOIS S., *Questioni sul fondamento costituzionale del diritto all'«identità personale» ,* in AAVV, *L'informazione e i diritti della persona*, Jovene, Napoli, 1983

GIAMPICCOLO G., *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza,* in *Riv. Trim. dir. Proc. Civ.,* 1958, 3 465

FONDAROLI C., *La tutela penale dei "beni informatici"*, in Il diritto dell'informazione e dell'informatica, 1996, 2, 311

FUMU G., *L'intercettazione di conversazioni domiciliari nella giurisprudenza di legittimità,* in *Studi sul processo penale in ricordo di Assunta Mazzarra,* CEDAM, Padova, 1996

GALDIERI P., *Il trattamento illecito del dato nei "social network",* in *Giurisprudenza di merito,* 2012, 12, 2699

GALDIERI P., *L'introduzione contro la volontà del titolare fa scattare la responsabilità dell'hacker*, in *Guida al diritto*, 2001, 1, 44

GALDIERI P., *Teoria e pratica nell'interpretazione del reato informatico*, Giuffrè, Milano, 1997

GARGIULO R.,*sub art. 617 quinquies*, in *Comm. LATTANZI-LUPO*, XI, 2, p. 1517

GIANNANTONIO E., *Manuale di diritto dell'informatica,* CEDAM, Padova, 1994

GAROFOLI R., *Manuale di diritto penale, parte speciale*, II, Roma, 2009

GRASSO, *L'anticipazione della tutela penale: i reati di pericolo ed i reati di attentato*, in *Riv. it. dir. proc. pen.*, 1986, 4, 689

GROSSO C. F., *Introduzione al diritto penale e alla politica criminale*, in *Manuale di diritto penale: parte generale*, Milano, Giuffrè Editore, 2013

HARLAN, *A reconsideration of the Katz Expectation of Privacy Test, in* 76 *Michigan Law Review,* University of Michigan, 1977

HASSEMER, *Il bene giuridico nel rapporto di tensione tra Costituzione e diritto naturale*, in *Dei delitti e delle pene*, 1984

IMPERIALI R., *Codice della Privacy,* Il sole 24 ore Pirola, Firenze, 2004

KOHLER G., *Das Autorrecht,* in *Iherings Jahrbucher,* XVII, 1880

KURZWEIL R., *La singolarità è vicina,* Apogeo, 2008

LA CUTE G., *Il dissenso presunto nel reato di violazione di domicilio*, in *Riv. Pen*., 1989, 6, 1041

LATTANZI G. a cura di, *Reati e responsabilità degli enti,* AA.VV., Giuffrè, Milano, 2005;

LOTIERZO, *Il caso Google – Vivi Down quale emblema del difficile rapporto degli internet* providers *con il codice della privacy,* in *Cass. pen.,* 2010, 1, 11

LOTIERZO R., *Del nocumento nell'illecito trattamento dei dati personali ovvero dell'esigenza di ascendere alle origini di una incriminazione,* in *Cassazione penale,* 2013, 4, 1593

LUBERTO M., *I reati informatici contro il diritto alla privacy. La tutela fornita dal D.lg. n.196 del 2003 e dal Codice Penale,* in *Giurisprudenza di merito,* 2008, 3, 900

LUCENTE C., *La nuova normativa penale a tutela dei dati personali,* in CARDARELLI-SICA-ZENO ZENOCOVICH, *Il codice dei dati personali. Temi e problemi,* Milano, 2004

LUCENTE C., *Sanzioni penali e amministrative a tutto campo per aumentare la tutela del cittadino,* in *Guida al diritto,* 1997, 4, 82

LUCENTE C., *Informatica e diritto penale: elementi per una comparazione con il diritto statunitense*, in *Diritto dell'informazione e dell'informatica*, 1987

LUCENTE, *I reati di accesso abusivo e danneggiamento informatico*, Relazione al seminario su I reati informatici, Roma, consultato 16.08.2014, in http://www.giustizia.it/

LUSITANO D., *In tema di accesso abusivo a sistemi informatici o telematici,* in *Giurisprudenza Italiana,* 1998, 5, 1924

MAGGIORE G., *Diritto penale – Parte Speciale,* Vol. II., Zanichelli, 1950

MAIORANO N., *sub art. 615 quater*, in PADOVANI T. a cura di, *Codice Penale*, 2007

MANNA A., *La prima affermazione a livello giurisprudenziale della responsabilità penale dell'internet provider: spunti di riflessione tra diritto e tecnica,* in *Giur. Cost.,* 2010, 2, 1856

MANNA A., *La protezione personale dei dati personali nell'ordinamento italiano,* in *Rivista trimestrale di diritto penale dell'economia,* 1993, 1, 188

MANNA A., *Il quadro sanzionatorio penale ed amministrativo del codice sul trattamento dei dati personali,* in *Il diritto dell'informazione e dell'informatica,* 2003, 4-5, 727

MANTOVANI F., *Diritto Penale – Parte Speciale, delitti contro la persona,* Cedam, Padova, 2012

MANTOVANI F., voce *Colpa*, in *Digesto di diritto penale,* Utet, Torino, 1988, vol. II

MANTOVANI F., *Diritto penale. Parte speciale I. Delitti contro la persona,* Cedam Padova, 1995

MANTOVANI F., *Diritto penale. Parte speciale I. Delitti contro la persona,* Cedam, Padova, 2011

MANTOVANI F., *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in AAVV, *Il diritto alla riservatezza e la sua tutela penale*, Milano, Giuffrè, 1970

MANZINI V., *Trattato di diritto penale italiano,* vol. VIII, n.3153, UTET, Torino, 1986

MARINI G., *Lineamenti del sistema penale*, Giappichelli, Milano, 2008

MARINUCCI G., "societas punir ipotest": *uno sguardo sui fenomeni e sulle discipline contemporanee,* in *Rivista italiana di procedura penale*, 2002, 5, 1193

MARINUCCI, DOLCINI, *Manuale di diritto penale, Milano*, 2012

MASI G., Frodi *informatiche e attività bancaria*, in *Rivista di politica economica*, 1995, 2, 428

MAZZA' P., *Considerazioni sul reato di divulgazione di notizie ed immagini attinenti alla vita privata,* in *Giurisprudenza di merito*, 1984, 4, 743

MILITELLO V., *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni,* in *Rivista trimestrale di diritto penale dell'economia,* 1992, 3, 374

MITNICK K., *L'arte dell'inganno*, Feltrinelli, Roma, 2003

MOCCIA E., *dalla tutela di beni alla tutela di funzioni: tra illusioni postmoderne e riflussi illiberali,* in *Riv. It. Di dir. e proc. Pen.,* 1995, 1, 343

MODUGNO F., *I nuovi diritti nella giurisprudenza costituzionale,* Torino, 1995

MONACO L., *Sub art. 615 bis c.p.,* in *Commentario breve al codice penale,* a cura di CRESPI, STELLA, ZACCALA', 4° Ed., Padova, 2003

MONACO L., *Sub art. 615 ter c.p.,* in *Commentario breve al codice penale,* a cura di CRESPI, STELLA, ZACCALA', 4° Ed., Padova, 2003

MONACO L., *Sub art. 615 quinquies c.p.,* in *Commentario breve al codice penale,* a cura di CRESPI, STELLA, ZACCALA', 4° Ed., Padova, 2003

MORSELLI E., *In tema di concezione realistica,* in *Problemi generali di diritto penale,* a cura di Vassalli, Giuliano, Giuffrè, Milano, 1982

MORSILLO G., *La tutela penale del diritto alla riservatezza*, Milano, Giuffrè, 1966

MUCCIARELLI F., voce Computer *(disciplina giuridica del) nel diritto penale,* in *Digesto delle discipline penalistiche,* vol II, Torino, 1988,

MUCCIARELLI F., *Commento all'art. 4 della legge 547 del 1993*, in *L'indice penale*, 1996, 1, 102

MUSACCHIO V., *Violazione di domicilio*, in *Digesto pen*., XV, Torino, 1999, 228

MUSCO E., MASULLO M. N., *I nuovi reati societari*, Giuffrè Editore, Milano, 2007

PADOVANI, *Diritto penale della prevenzione e mercato finanziario*, in *Rivista it. Dir. proc. Penale*,1995, 1, 81

PAGLIARO A., *Bene giuridico e interpretazione della legge penale,* in *Studi in onore di Francesco Antolisei,* Volume II, Giuffrè. Milano, 1965

PAGLIARO A., *Bene giuridico e interpretazione della legge penale,* in *Studi in onore di F. Antolisei*, II, Milano, 1965

PALAZZO F.C., *Considerazioni in tema di tutela della riservatezza (a proposito del nuovo art. 615 bis c.p.),* in *Rivista italiana di diritto e procedura penale*, 1975, 1, 130

PALIERO, *Consenso sociale e diritto penale*, in *Riv. it. dir. proc. pen*., 1992, 3, 915

PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali,* Milano, 2003

PARODI GIUSINO, *I reati di pericolo tra dogmatica e politica criminale,* Milano, 1990

PARODI C., CALICE A., *Responsabilità penali e internet*, IlSole24Ore, Milano, 2001

PALAZZO F.C., *Bene giuridico e tipi di sanzione,* in *Indice Penale,* 1992, 1, 213

PATALANO, *Significato e limiti della dommatica del reato di pericolo,* Napoli, 1975

PATRONO P., voce *Privacy e vita privata (dir. pen.)*, in *Enciclopedia del diritto,* Vol. XXXV, Milano, 1986

PAZIENZA P., *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547*, in *Rivista italiana di diritto e procedura penale*, 1995, 3, 750

PECORELLA G., *Profili penalistici della regolamentazione delle banche dati,* in *AA. VV., Le banche dati in italia. Realtà normativa e progetti di regolamentazione* (a cura di V. Zeno-Zencovich), Napoli, 1985

PECORELLA G., *Il diritto penale dell'informatica,* Cedam, Padova, 2000

PECORELLA G., *Il diritto penale dell'informatica*, Cedam, Padova, 2a ed., 2006

PECORELLA G., *sub. Art. 392*, in MARINUCCI-DOLCINI, *Codice penale commentato,* IPSOA, Milano, 2011

PECORELLA G., *sub. Art. 615 ter*, in MARINUCCI-DOLCINI, *Codice penale commentato,* IPSOA, Milano, 2011

PECORELLA G., *sub. Art. 615 quater*, in MARINUCCI-DOLCINI, *Codice penale commentato,* IPSOA, Milano, 2011

PECORELLA G., *sub art. 615 quinquies,* in MARINUCCI-DOLCINI, *Codice penale commentato,* IPSOA, Milano, 2011, pag. 6001

PECORELLA G., *Dieci anni di giurisprudenza sui reati informatici: i principali problemi interpretativi sollevati dalle nuove disposizioni*, in *Cocco,Interpretazione e precedente giudiziale in diritto penale*, Padova, 2005

PEDRAZZI C., *I reati fallimentari,* in PEDRAZZI e AA.VV., *Manuale di diritto penale dell'impresa,* Bologna, 1999

PERREAU V., *Les droits de la personnalite, in Rev. Trim. d. Civ.,* Parigi, 1909

PICA G., *Diritto penale delle tecnologie informatiche,* UTET, Torino, 1999

PICA G., *Diritto penale delle tecnologie informatiche,* UTET, Torino, 1997

PICOTTI L., *I diritti fondamentali nell'uso ed abuso dei social network: aspetti penali,* in *Giurisprudenza di merito,* 2012, 12, 2532

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004

PICOTTI L., *Profili di diritto penale sostanziale*, in *La ratifica della Convenzione sul Cybercrime del Consiglio d'Europa*, in *Diritto penale e processo*, 2008, 3, 710

PICOTTI L., *La ratifica della convenzione cybercrime del consiglio d'Europa,* in *Diritto penale e processo*, 2008, 6, 696

PIERGALLINI C., *Sistema sanzionatorio e reati previsti dal codice penale,* in *Diritto penale e procedura,* 2001, 6, 1365

PISTORELLI L., *Relazione di Cassazione n. III/01/2013,* 28 agosto 2013, p. 7

POMANTE G., *Internet e criminalità*, Giappichelli, Torino, 1999

PROSSER W.L., *Privacy, a legal analysis,* in *California Law Review,* 1960, 48, 383

PUGLIESE G., *Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche,* in *Foro Italiano*, Zanichelli, Bologna, 1954, 1, 118

PULITANO' P., *La responsabilità da "reato" degli enti: i criteri d'imputazione*, in *Rivista italiana di diritto e procedura penale,* 2002, 3, 420

RAMACCI L., *Diritto penale dell'ambiente,* CEDAM, Padova, 2009

RAVA' A., *I diritti sulla propria persona nelle scienza e nella filosofia del diritto,* Torino, 1901

RAVA' A., *Istituzioni di diritto privato,* Cedam, Padova, 1938

RESTA P., *Cybercrime e Cooperazione Internazionale nell'ultima legge della legislatura*, in *Giurisprudenza di Merito*, 2008, 1, 5

REVERDITI M., *La responsabilità degli enti: la crocevia fra responsabilità da reato degli enti collettivi,* Giuffrè, Milano, 2009

RODOTA' S., *Intervista su privacy e libertà,* a cura di Paolo Conti, Editori Laterza, Roma-Bari, 2005

RODOTA' S., *Tecnologie e diritti*, Bologna, Il Mulino, 1995

RONCO M., *Vita privata (interferenze illecite nella)*, in *Novis, Digesto It.*,VII, UTET, Torino, 1987, 163

ROSSI V., *Divieto di controllo a distanza e telelavoro,* in *Codice in materia di protezione dei dati personali,* Vicenza, 2004

ROSSI VANNINI A., *La criminalità informatica: le tipologie di computer crimes di cui alla L.547/93 diretta alla tutela della riservatezza e del segreto,* in *Rivista trimestrale di diritto penale dell'economia,* 1994, 2, 436

RUGGIERO C., *Capacità penale e responsabilità degli enti,* Giappichelli, Torino, 2004

SALVI R., *La Corte di Cassazione sul caso Google vs Vivi Down: l'host provider non governa il mare magnum della rete,* in *Diritto civile e commerciale,* in *Diritto.it*, 2014, consultato il 16/07/14, http://www.diritto.it/docs/36069-la-corte-di-cassazione-sul-caso-google-vs-vivi-down-l-host-provider-non-governa-il-mare-magnum-della-rete?page=1

SANDULLI A.M., BALDASSARRE A., *Profili costituzionali della statistica in Italia*, in *Dir. soc*., 1973

SANTORIELLO C., *Un osservazione sul Decreto Legge 93/2013,* in *Rivista 231,* 2013, consultato in Agosto 2014, http://www.rivista231.it/Legge231/Pagina.asp?Id=933

SANTORIELLO C., *Una ulteriore osservazione sul Decreto Legge 93/2013,* in *Rivista 231,* 2013, consultato in Agosto 2014, http://www.rivista231.it/Legge231/Pagina.asp?Id=942.

SARZANA C., IPPOLITO S., *La legge di ratifica della Convenzione id Budapest: una gatta legislativa frettolosa*, in *Diritto e procedura penale*, 2008, 7, 1562

SGUBBI, FONDAROLI, TRIPODI, *Diritto penale del mercato finanziario,* II edizione, CEDAM, Padova, 2013

SICA S., *Danno e nocumento nell'illecito trattamento di dati personali,* in *Il diritto dell'informazione e dell'informatica*, 2004*,* 4-5, 714

SINISCALCO E., *Domicilio* (violazione di), in ED, XIII, Milano, 1964

SIRACUSA L., *La tutela penale dell'ambiente: bene giuridico e tecniche di incriminazione,* Milano, Giuffrè Editore, 2007

SOFOCLE, *Edipo re – Edipo a Colono – Antigone*, a cura di Dario Del Corno, Oscar Mondadori, 2006

SPAGNOLO N. a cura di, *La responsabilità da reato degli enti collettivi. Cinque anni di applicazione del d.lgs. 8 giugno 2001 n. 231,* AA.VV., Giuffrè, Milano, 2007

VASSALLI C., *Libertà di stampa e tutela penale dell'onore* in *Archivio penale,* 1967

TRONCONE P., *Il delitto di trattamento illecito di dati personali,* Giappichelli, Torino, 2011

VENEZIANI P., in *I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali,* tratto da *Il diritto penale dell'informatica nell'epoca di internet,* a cura di PICOTTI L., Cedam, Padova, 2004

VENEZIANI P. *Beni giuridici protetti e tecniche di tutela penale,*in *Rivista trimestrale di diritto penale dell'economia,* 1997, 1, 144

VIGNA L., DUBOLINO P., *Segreto*, in ED, XLI, Milano, 1989, 1079

VILLANI C., *Il codice del trattamento dei dati personali,* a cura di CUFFARO-D'ORAZIO-RICCIUTO, Giappichelli, Torino, 2006

VINCIGUERRA S., *Quale specie di illecito,* in VINCIGUERRA-CERESA GASTALDO-ROSSI, *La responsabilità dell'ente per il reato commesso nel suo interesse,* Cedam, Padova, 2004

WESTIN A., *Privacy and Freedom,* Atheneum, New York, 1970

ZAGREBELSKY V., *La convenzione europea dei diritti umani, la responsabilità delle persone morali e la nozione di pena,* in AA.VV., *Responsabilità degli enti,* 31

ZENO-ZENCOVICH, V., *"Personalità (diritti della)"*, in *Digesto delle discipline penalistiche*, 1995

ZUCCALÀ G., *Due questioni attuali sul bene giuridico: la pretesa di dimensione critica del bene e la pretesa necessaria offesa ad un bene,* in *Riv. Trim. dir. pen. Ec.,* 2004, 4, 839

ZWEIGERT K., KOTZ H., *Introduzione al Diritto Comparato,* volume II, Giuffrè, Milano 1995