QUESITI

PASQUALE TRONCONE

La rilevanza penale del trattamento dei dati personali

La riforma del Codice della tutela dei dati personali, dopo l'entrata in vigore del Regolamento europeo nel 2018, ha comportato due importanti novità. In primo luogo, il riconoscimento nella legislazione penale della riservatezza della persona come interesse autonomo meritevole di tutela. Ne è seguita una profonda rivisitazione della parte relativa alle norme penali, con l'introduzione di nuove figure di reato e un più significativo ruolo del Garante della Privacy in materia processuale.

The criminal relevance of the processing of personal data and the new punitive strategy

The reform of the Personal Data Protection Code, after the entry into force of the European Regulation in 2018, resulted in two important changes. In the first place, a change of a dogmatic character which registered for the first time in criminal legislation the legislative recognition of the confidentiality of the person. This was followed by a profound review of the part relating to criminal law, with the introduction of new crime figures and a new and more significant role of the Privacy Authority in procedural matters.

1. *Premessa*. Com'è noto, a distanza di quindici anni dall'introduzione del reato di trattamento illecito di dati personali prevista all'art. 167 del d. lgs. n. 196 del 2003 ed a seguito delle nuove sollecitazioni provenienti dal diritto sovranazionale, il legislatore italiano nel 2018 è nuovamente intervenuto in materia di *privacy* arricchendo il quadro delle scelte sanzionatorie di natura penale.

La spinta evolutiva della materia impressa dal diritto convenzionale è ravvisabile nel fatto che il legislatore nazionale si è posto il problema del "doppio binario" sanzionatorio rispetto a taluni comportamenti qualificabili contestualmente come illecito amministrativo e come illecito penale, risolvendolo

senza incorrere nella violazione del principio regolatore di garanzia del *ne bis in idem*.

Tuttavia, la novità più rilevante è fornita da una vera e propria trilogia punitiva di carattere strettamente penale in materia di trattamento illecito di dati, dal momento che il d. lgs. n. 101 del 10 agosto 2018 innesta nel tessuto connettivo dell'apparato punitivo due nuove di figure di reato, procedendo anche a una modifica strutturale del precedente art. 167 del codice della privacy (di seguito: CdP), dove ha insediato una ulteriore terna di reati.

La gestazione delle nuove norme penali è stata piuttosto complessa, considerato che nella prima stesura del decreto legislativo era stata eliminata del tutto la parte sanzionatoria penale, con la decisa abrogazione dell'art. 167 CdP. Rispristinata successivamente dalle Commissioni parlamentari in sede di pareri è stata addirittura ampliata offrendo l'immagine di un autentico baluardo punitivo, con l'art. 167-*bis* CdP e poi l'art. 167-*ter* CdP[1].

Questo nuovo assetto normativo estende notevolmente il campo della tutela penale, non solo di questo settore ma di tutto l'ampio ventaglio della categoria dei reati informatici, e, d'altro lato, allinea la nostra legislazione alle fonti sovranazionali.

Il legislatore italiano, infatti, come sovente accaduto negli ultimi anni, ha subito la spinta di interventi normativi di fonte europea[2] che hanno improvvisamente mutato il quadro dell'originario assetto del D.Lgs. n. 196 del 2003[3].

La materia del trattamento di dati ha registrato, occorre subito osservarlo, una notevole dilatazione regolativa, a seguito dell'entrata in vigore di provvedimenti legislativi di portata diversa che hanno finito per minare alla base la struttura sistematica che rendeva più agevole il compito all'interprete[4].

Venuto meno il principio di coerenza e di sintesi oggi lo sforzo di ricercare la regola del caso e la sua tutela ovvero la punibilità nell'ipotesi della sua viola-

---

[1] Si rinvia sul punto agli interventi in Parlamento presso le Commissioni competenti del Garante della *privacy*, Dott. Antonello Soro, del 26 novembre 2015 e del 7 giugno 2018, in *www.parlamento.it*.

[2] ATERNO, CORASANITI, CORRIAS LUCENTE, *L'attuazione della Convenzione europea su cybercrime. Commento alla legge 18 marzo 2008 n. 48*, Padova, 2009. PICOTTI, *La ratifica della Convenzione europea sul Cybercrime del Consiglio d'europa. Profili di diritto penale sostanziale*, Padova, 2008. Sul tema, in maniera ampia e aggiornata, si rinvia al ponderoso volume *Cybercrime*, a cura di Cadoppi, Canestrari, Manna, Papa, Torino, 2019.

[3] PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016.

[4] RESTA F., *I reati in materia di protezione dei dati personali*, in *Cybercrime cit.*, 1019. Il recente inserimento della categoria dei delitti informatici nell'art. 24-*bis* del D.Lgs n. 231 dell'8 giugno 2001, avvenuto per effetto del D.Lgs. n. 75 del 14 luglio 2020, conferma che l'ampliamento della base della punibilità, questa volta come sanzione comminata all'Ente, corrobora il ruolo centrale che hanno assunto queste nuove figure di reato.

zione, mette a dura prova lo strumento esegetico. L'esigenza di coordinare senza un ordine sistematico una complessa materia che da sempre si è nutrita di numerose ipotesi di rinvio recettizio e di norme penali in bianco, presta ancor di più il fianco all'incertezza applicativa. Non solo. La perdita del quadro di sistema mette alle corde anche lo sforzo legislativo per rendere utile la razionalità definitoria che il legislatore del 2003 aveva adottato con le disposizioni poste ad esordio del primo Codice del trattamento. Era stata salutata con favore, infatti, la scelta di aprire il documento normativo con una serie di norme che definivano in maniera incontrovertibile le condotte di trattamento, gli ambiti di intervento e le operazioni oggetto del trattamento dati.
Le ultime vicende della pandemia da COVID-19 hanno enfatizzato in maniera ancora più decisa il ricorso agli strumenti informatici e allo scambio delle informazioni che riguardano la vita privata della persona imponendo un innalzamento del tasso di protezione e di prevenzione degli stessi.

2. *Uno sguardo d'insieme al nuovo assetto normativo*. Una preliminare osservazione del nuovo impianto sanzionatorio riguarda la natura degli illeciti che passano dalla graduale gravità di violazioni amministrative, previste e contenute in un diverso provvedimento legislativo - il Regolamento europeo -, a fattispecie penali[5]. Molto spesso, come più avanti vedremo, si è determinata una vera e propria sovrapposizione punitiva, con il rischio di raddoppiare la sanzione per lo stesso fatto, esito ora sventato da una specifica norma che il legislatore italiano ha introdotto per risolvere il raddoppio di penalità.
Il profilo più rilevante sul piano penale è la previsione di una trilogia di fattispecie penali che si aggregano intorno ad un unico concetto finalistico, il profitto, seppure dettagliate negli elementi tipicità da circostanze costitutive del tutto diverse. Si avvia un nuovo percorso di valore, poiché emerge chiaramente l'impossibilità di obliterare esigenze di tutela della riservatezza che dall'entrata in vigore del Codice del trattamento del 2003 veniva da più parti invocato. Il nuovo fronte di indagine giuridica vede, infatti, al centro della portata innovativa del Codice la tutela della riservatezza come nozione giuridica nota alla dottrina tradizionale, ma inizialmente filtrata attraverso la "identità informatica" che ogni persona fisica acquisisce allorchè accede alla Rete e vi opera al suo interno. Peraltro, le operazioni compiute ricevono in prima

[5] BOLOGNINI, PELINO, BISTOLFI, *Il regolamento privacy europeo. Commentario alla nuova disciplina*, Milano, 2016. AA.VV., *Protezione e libera circolazione dei dati personali nel diritto europeo. Il Regolamento generale 2017/679 (e le Direttive 2016/680 e 2016/681 sul trattamento dei dati in ambito penalistico)*, a cura di D'Orazio e Ricciuto, Torino, 2017.

battuta una tutela che mira a salvaguardare i procedimenti di trattamento che abbiano come finalità unica ed esclusiva il profitto, dunque le operazioni commerciali effettuate in Rete.
A questo punto, una lettura più attenta e attuale della norma disvela una potenzialità ermeneutica diversa, indirizzata, seppure imprevedibilmente, alla tutela della dignità della persona. Il quadro dei principi fondamentali di orientamento e le rinnovate fonti ordinarie eurounitarie depongono in questo senso.
Originariamente il problema del trattamento dei dati identificativi delle persone emerge all'attenzione del legislatore con la Direttiva 95/46 "*Privacy Directive*", adottato sulla base dell'art. 95 del precedente *Trattato della Comunità Europea* in quanto chiamato a garantire la creazione e il rafforzamento del mercato interno attraverso la certezza giuridica e operativa delle persone. Quindi, già nella sua fase genetica la materia del trattamento dati assumeva una dimensione concettuale di tipo economico e una fisionomia normativa del tutto autonoma e ben definita.
Nulla sembrava riguardare le circostanze di vita relative a una persona, i suoi rapporti, le sue relazioni, il suo agire privato, questi sono semplicemente fatti, oggetto sì di riservatezza, apparentemente del tutto al di fuori e avulsi della portata protettiva del Codice del trattamento di dati identificativi della persona fisica[6].
In questo nuovo quadro normativo il legislatore si è proposto una prospettiva, quella di qualificare in maniera autonoma illeciti penali che mostrassero obiettivi punitivi diversi, chiaramente ambivalenti, con elementi specializzanti che rendessero distinte le fattispecie e più agevole il compito alla sede applicativa.
Non mancano naturalmente obiezioni. Per esempio, suscita perplessità la parcellizzazione dei fatti che finiscono per rifrangersi sull'ambiguità di elementi costitutivi del reato la cui natura resta di incerta determinazione concettuale.
Diversamente da quanto avviene negli ultimi tempi, questa volta il legislatore italiano ha indicato nella rubrica dei rispettivi tre reati una sintetica descrizione molto precisa capace di orientare l'interprete[7].

[6] In realtà era stato puntualmente intuito il nuovo percorso da MANNA, *Tutela penale della personalità*, Bologna, 1993.
[7] Per l'ambigua formulazione del lessico delle rubriche, si rinvia alla riflessione di SOTIS, *Vincolo di rubrica e tipicità penale*, in *Riv.it.dir. e proc.pen.*, 2017, 1362.

Il Capo II è dedicato alle norme penali e l'art. 167 CdP esordisce con una disposizione che raccoglie la precedente previsione incriminatrice ampliandone la base applicativa e rubricandola "*Trattamento illecito di dati*".
Il successivo art. 167-*bis* CdP reca in rubrica "*Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala*" che agevolmente rimanda a una modalità specifica e che ne costituisce il profilo di specialità.
La terza disposizione, infine, rubricata all'art. 167-*ter* CdP "*Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*" assolve a un fine estraneo al trattamento dei dati e ricopre una condizione di reato ostacolo e prodromico.
Occorre subito precisare che le tre disposizioni non contengono tre ipotesi di reato, ma molto di più e l'incauto assemblaggio per "genere", di fatto, ne rende ancora più accidentata la lettura e la qualificazione dei singoli elementi costitutivi.
Il comune denominatore della complessiva disciplina, peraltro, ruota intorno alla clausola di sussidiarietà che rende i fatti suscettibili di applicazione succedanea rispetto a disposizioni incriminatrici più significative e contrassegnate da un carico sanzionatorio superiore.
In realtà questo modo di disciplinare la fattispecie ne depotenzia l'efficacia, perché il solo diverso indice di gravità è tale da assorbire la punibilità del fatto da un ambito di tutela e una categoria di bene giuridico del tutto diverso da quello originario. Ma su questo aspetto torneremo più avanti.

3. *La disciplina multilivello e integrata nel contesto continentale. Esigenza di una comune base giuridica.* Vi è una petizione di principio che non può sfuggire in sede esegetica, perché contribuisce a comprendere come mai il tema del trattamento dei dati sia stato rifratto in tre diversi documenti legislativi. Infatti, accanto al Regolamento europeo e al Codice D.Lgs. n. 196/2003 compare un nuovo D.Lgs. n. 51 del 2018, con diverse fattispecie penali.
Sembra quasi che le Autorità normative europee abbiano con ansia avvertito la necessità, non solo di dotare gli stati dell'Unione di una legislazione comune ed omogenea, ma anche di fornire una disciplina a tal punto solida ed esauriente tale da sottrarre agli altri formanti del diritto sovranazionale la possibilità di intervenire con decisioni creative. In altri termini il perfetto ordine sistematico che presenta con una legislazione ricca e fitta dovrebbe impedire il disordine che potenzialmente potrebbe essere generato da disposizioni dal contenuto generico e affidato nel dettaglio ai singoli stati nazionali.

Questa inedita tecnica è in realtà utile a sottrarre potere di normazione integrativa ai parlamenti nazionali, con tutte le conseguenze, positive e negative, che ciò comporta.
Resta il fatto che da un punto di vista tecnico, al di là della sconfinata disciplina messa in campo, lo spazio per una giurisprudenza creativa appare realmente ridotto o addirittura annullato. Non manca, peraltro, la ricaduta di valore di una tale scelta legislativa che è nel senso di dare piena operatività e, allo stesso tempo, legittimazione unica alla legalità dell'Unione. Ambito in cui si raccolgono e si raccordano le scelte uniformi di regolazione dei rapporti giuridici e delle relazioni tra soggetti, evitando di offrire spunti e spazi di scelte indipendenti che potrebbero minare il proposito di unitarietà del progetto continentale.
Bisogna riconoscere che la materia del trattamento dei dati personali, sommariamente definita *privacy*, rappresenta uno dei modelli di coesione di riferimento per le fonti comuni del diritto che l'Unione europea ha coltivato fin dalla sua istituzione.
Alcune Carte costituzionali di paesi membri ne prevedono esplicitamente la protezione -come quella spagnola-, così come la tutela è prevista in linea generale dall'art. 16 del *Trattato del funzionamento dell'unione europea* come modificato dal Trattato di Lisbona.
Questa volta, rispetto anche ad un recente passato, scendono in campo diverse fonti del diritto che variamente, secondo il sistema multilivello, trovano collocazione operativa seppure in termini di interferenza[8]. Si tratta dei sistemi normativi costituzionale interno, eurounitario e convenzionale, le cui espressioni operative sono le Corti costituzionali nazionali, la Corte GUE e la Corte EDU, quest'ultime come giudici che producono diritto e, in un costante e fruttuoso dialogo, arricchiscono le fonti legislative esistenti[9].
Pur nella variegata vigenza delle norme fondamentali e dei principi di riferimento nel nostro ordinamento, anche per quanto si vedrà più innanzi, il trattamento dei dati personali ritrova il suo referente di valore non più come in origine nell'art. 2 e poi nell'art. 21 della nostra Carta fondamentale, ma per il

[8] CONTI, *Il sistema di tutela multilivello e interazione tra ordinamento interno e fonti sovranazionali*, in *Quest.giust.*, n. 4, 2016.
[9] POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *www.federalismi.it*. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Gli artt. 7 e 8 della Carta di Nizza nel reasoning di Google spain*, in *Dir.dell'inf. e dell'inf.*, n. 4-5, 2014. PREVOSTI, *Tutela della privacy come presupposto della libertà: due recenti sentenza della Corte di Giustizia dell'unione Europea a difesa della riservatezza individuale*, in *www.osservatorioaic.it*, settembre 2014.

riposizionamento concettuale subìto nel corso degli anni, la radice trova il suo indirizzo di orientamento della disposizione dell'art. 15 Cost., laddove è stabilito che: "*La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili*".
A livello normativo la materia del trattamento dei dati ha avuto la sua origine con il primo intervento normativo organico nella storia della legislazione italiana, che teneva conto della necessità di tutelare in modo specifico i dati identificativi della persona, della legge 21 febbraio 1989 n. 98 che ratificava la Convenzione di Strasburgo n. 108 del 28 gennaio 1981[10].
Le direttive succedutesi nel tempo hanno originato negli ordinamenti nazionali tre fondamentali leggi che in Italia sono state la n. 675 del 31 dicembre 1996/95, in cui la fattispecie penale viveva ancora in una sorta di ambigua posizione tra tutela della persona e tutela dei dati[11]. A sciogliere il nodo e soprattutto a dare piena attuazione ai provvedimenti normativi sovranazionali interviene poi il D.Lgs. n. 196 del 2003 denominato "*Codice per il trattamento di dati personali*" che conferisce una struttura esauriente e organica a tutta la materia.
L'esigenza di maggiore coesione e di razionalizzazione del sistema delle regole del mercato europeo, anche per inserirsi in maniera compatta con una disciplina uniforme nello scenario del commercio internazionale, ha fatto registrare la necessità di varare una regolamentazione giuridica unitaria per tutti gli stati nazionali europei. Ecco che viene varato il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 ed entrato in vigore in tutta l'Unione Europea il 25 maggio 2018, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
Va precisato che il Regolamento prevede nel suo apparato sanzionatorio la punibilità unicamente degli illeciti amministrativi, non esiste alcuna previsione

[10] MILITELLO, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv.trim.dir.pen.econ.*, 1992. PECORELLA, *Il diritto penale dell'informatica*, Padova 2000.
[11] BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997. PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 281. MANNA, *La protezione penale dei dati personali nel diritto italiano*, in *Riv.trim.dir.econ.*, 1997, 179 e ss. MANTOVANI, *Le fattispecie incriminatrici sulla privacy: alcuni spunti di riflessione*, in *Crit.dir.*, 1997, n. 4, 194. SEMINARA, *Appunti in tema di sanzioni penali nella legge sulla* privacy, in *Resp.civ. e prev.*, 1998, 912. VALASTRO, *La tutela penale delle comunicazioni intersoggettive, fra evoluzione tecnologica e nuovi modelli di responsabilità*, in *Riv.it.dir. e proc.pen.*, 1999, pag. 989. DEL CORSO, *Commento alle sanzioni penali della l. 31 dicembre 1996, n. 675*, in *Le nuove leggi civ.comm.*, 1999, 728. AA.VV., *La giustizia penale nella rete. Le nuove sfide della società dell'informazione nell'epoca di Internet*, a cura di Flor, Falcinelli, Marcolini, Milano, 2015.

di fattispecie penali. Probabilmente questa scelta è stata indotta dal fatto che negli stati nazionali il principio generalmente vigente in materia penale è quello della riserva di legge e dove vige la garanzia di fonte alta della stretta legalità per cui può intervenire a legiferare norme repressive soltanto il Parlamento di quel paese.
Il richiamo al principio di proporzionalità della opzione legislativa penale appare particolarmente importante, perché impone l'adozione del canone comune sancito all'art. 49 della Carta dei diritti Fondamentali dell'Unione europea, proclamata a Nizza il 7 dicembre 2000, che riveste lo stesso valore giuridico dei Trattati, in forza dell'art. 6, comma 1, del Trattato sull'Unione Europea (TUE), come modificato dal Trattato di Lisbona, firmato il 13 dicembre 2007, ratificato e reso esecutivo con legge 2 agosto 2008 n. 130, ed entrato in vigore il 1° dicembre 2009 "*Principi della legalità e della proporzionalità dei reati e delle pene*"[12].
Il Regolamento europeo, insomma, appare decisivo anche per stabilire in via definitiva quale sia il vero interesse giuridico tutelato dalla legge e, per quanto concerne le norme penali, quale sia il bene che la fattispecie incriminatrice intende proteggere. Seppure il diritto sovranazionale ha ridimensionato il ruolo della teoria del bene giuridico, resta essenziale la sua funzione classificatoria e in questo specifico caso l'individuazione normativa del bene protetto fa fuoriuscire dal cono d'ombra il vero obiettivo di protezione.
Ormai il Regolamento europeo ha scolpito il vero scopo della legge quando ha stabilito al Capo I "*Disposizioni generali*" - Articolo 1 "*Oggetto e finalità*": "*1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè norme relative alla libera circolazione di tali dati. 2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. 3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*".

4. *La clausola normativa per rispettare il principio di garanzia convenzionale del* ne bis in idem. La disciplina di indirizzo di stampo europeo contiene una serie di indicazioni vincolanti per gli stati nazionali. Vincoli che riguardano l'obbligo di normazione di specifici settori e criteri di operatività, ma non vin-

[12] AA.VV., *I diritti fondamentali dopo la Carta di Nizza. Il costituzionalismo dei diritti*, a cura di Ferrari, Milano, 2001. AA.VV., *I diritti fondamentali dell'Unione europea. La Carta di Nizza dopo il Trattato di Lisbona*, a cura di Gianniti, Bologna, 2013.

coli di contenuto, con la possibilità di prevedere disposizioni di maggior dettaglio e di adeguamento al nuovo sistema.
Sulle norme penali, al di là del criterio di proporzionalità, viene concessa la facoltà di dare vita alla produzione di norme penali secondo il criterio guida della c.d. "*finalità complementare*". Questo assetto in realtà delinea un "*sistema sanzionatorio integrato*" che svolge certamente una funzione di tutela di livello significativo, a condizioni però che le norme punitive dei diversi settori dell'ordinamento siano formulate in modo tale da esprimere quella efficacia auspicabile per la quale sono state progettate. Diversamente, più che rappresentare una ricchezza per la legislazione, la scelta di elaborare un sistema integrato di sanzioni corre il rischio di far convergere più norme sullo stesso fatto concreto, cumulandone ingiustificatamente gli effetti punitivi.
Si tratta di una inedita scelta di merito ma anche di metodo, soprattutto di strategia di politica criminale che, accanto al principio di *extrema ratio*, pone un'esigenza di carattere operativo devoluta ai singoli stati nazionali, quella che finisce per rappresentare una finalità non essenziale ma di tipo ausiliare, non necessaria ma opportuna.
Volendo trasferire questa ulteriore opzione penalistica nel nostro sistema dommatico si può affermare che in questo modo il diritto penale non svolge una funzione tesa soddisfare esigenze laddove non riescono altri settori dell'ordinamento, ma di esercitare invece opera di rafforzamento di quel settore già presidiato da norme punitive seppure di natura diversa. Non bisogna dimenticare che il diritto penale svolge una funzione repressiva ma soprattutto preventiva attraverso la pena e lo stigma che ne deriva nella sua applicazione al colpevole è tipico soltanto del diritto penale. Qualunque altra sanzione, seppure economicamente penalizzante, non reca con sè il carattere punitivo e riabilitativo tipico della sanzione penale.
Va salutata, inoltre, con favore l'iniziativa del legislatore di riconoscere piena efficacia ai principi di garanzia fondamentali della persona ed in particolare al divieto di applicare due sanzioni di natura diversa ad uno stesso fatto concreto.
La scelta, per la verità obbligata, deriva direttamente dal diritto eurounitario e giurisprudenziale che si va consolidando negli ultimi anni in Europa tra le Corti di Bruxelles e Strasburgo.
La nostra legislazione nazionale, benchè la dottrina abbia più volte avvertito del sospetto di illegittimità costituzionale della doppia sanzione, ha sempre trascurato di sciogliere il nodo della sovrapposizione tra sanzione penale e sanzione amministrativa. Probabilmente la rilevanza economica delle materie

interessate al fenomeno duplicativo del "doppio binario" impediva di intraprendere iniziative che avrebbero finito per depotenziare l'efficacia dissuasiva della legge.
Sia in materia tributaria che nelle leggi che regolano i mercati finanziari il fenomeno del doppio binario punitivo era caduto ormai sotto la lente di ingrandimento della giurisprudenza eurounitaria e convenzionale.
Un primo duro colpo per dare rilevanza al divieto del *ne bis in idem* era stato assestato dalla Corte EDU con la sentenza originata dal caso Grande Stevens[13] che, in materia di abusi di mercato, aveva ritenuto illegittimo la doppia sanzione, per poi vedere ridimensionare tale assunto con decisioni successive della giurisprudenza eurounitaria, in particolare con la decisione della Corte GUE nel caso C-573/16 *Garlsson Real Estate* e altri.
Il dibattito acceso sul divieto del doppio processo e della doppia sanzione ha trovato un primo punto di quiete con la sentenza della Corte costituzionale n. 43 del 2017 in materia tributaria che ha stabilito il principio per cui la garanzia del *ne bis in idem* va intesa nel senso di evitare la sproporzione sanzionatoria rispetto alla effettiva rilevanza del fatto concreto. In astratto le due misure sanzionatorie, illecito penale e illecito amministrativo, nella loro piena autonomia possono essere dunque adottate dal legislatore. Ciò che bisogna evitare è che in concreto, rispetto ai medesimi fatti, venga applicata una doppia sanzione pecuniaria, anche se resta fuori da quest'opera di contemperamento sanzionatorio la pena detentiva per evidenti ragioni di eterogeneità. Soprattutto quando, nella piena indipendenza di ciascun procedimento, tributario e penale, vi sia un lasso temporale e una diversità probatoria tale da escludere una piena sovrapposizione dei giudizi[14].
Sul punto il Regolamento europeo di protezione dei dati si presenta fondamentale per il canone che prescrive al n. 149 del Considerando: "*Gli Stati*

[13] CORTE EDU, Sez. II, 4 marzo 2014, *Grande Stevens e altri c. Italia*, con nota di TRIPODI, *Uno più uno (a Strasburgo) fa due. L'Italia condannata per violazione del* ne bis in idem *in tema di manipolazione del mercato*, in *www.penalecontemporaneo.it*.
[14] CORTE COST. Sent. n. 24 del 24 gennaio 2018, in *www.cortecostituzionale.it*, pag. 9: "*Questa Corte tiene a sottolineare che la nuova regola della sentenza A e B contro Norvegia rende meno probabile l'applicazione del divieto convenzionale di bis in idem alle ipotesi di duplicazione dei procedimenti sanzionatori per il medesimo fatto, ma non è affatto da escludere che tale applicazione si imponga di nuovo, sia nell'ambito degli illeciti tributari, sia in altri settori dell'ordinamento, ogni qual volta sia venuto a mancare l'adeguato legame temporale e materiale, a causa di un ostacolo normativo o del modo in cui si sono svolte le vicende procedimentali*". Tale orientamento ha ricevuto una prima applicazione, proprio in materia tributaria per evitare il rischio di sovrapposizione tra procedimento tributario e procedimento penale, da Cass., Sez. III, 6 luglio 2018, in *www.cassazione.it*.

membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento. Tuttavia, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di giustizia".

All'interno dell'articolato che segue, invece, si ritrova un'altra indicazione vincolante che il legislatore nazionale è stato tenuto a seguire con l'art. 84 "*Sanzioni*": "*1. Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie*".

Orbene, il legislatore italiano, se in un primo momento sembrava intendesse depenalizzare le vecchie fattispecie penali contenute nel D.Lgs. n. 196/2003, successivamente ha confermato in parte le preesistenti e ne ha introdotto di altre, sciogliendo il vincolo normativo sovranazionale e andando a coprire con la norma penale quella stessa area di punibilità che appartiene all'illecito amministrativo. Si tratta di punire, in sostanza, per il medesimo disvalore del fatto.

In realtà, non vi è alcun indirizzo vincolante delle leggi o del diritto giurisprudenziale che nega la possibilità di riconoscere allo stesso fatto concreto un doppio giudizio di disvalore, penale e poi amministrativo, viene soltanto stabilita la limitazione della misura della sanzione, per cui una delle due va ridotta in presenza della effettiva esazione dell'altra, secondo quanto stabilisce in criterio di carattere generale previsto all'art. 187-*terdecies* del "*Testo unico delle disposizioni in materia di intermediazione finanziaria (TUF)*".

Va detto che nella materia della riservatezza la rotta di collisione è stata evitata per effetto della disciplina regolatrice dell'art. 167 dell'attuale Codice del trattamento dei dati che al comma 6 stabilisce: "*Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita*".

La portata della disposizione non è trascurabile, perché prima di tutto si tratta di uno stesso fatto che deve intendersi "concreto", non in astratto come previsto dal precetto normativo. In secondo luogo, se anche si dovesse registrare una convergenza, per effetto della celebrazione contemporanea del doppio giudizio e per l'identità probatoria che li accomuna, una volta esatta la sanzio-

ne pecuniaria, la pena, in questo caso come vedremo solo detentiva, deve essere diminuita.
In altri termini, in relazione al disvalore del fatto concreto, essendo comune ad entrambe le iniziative sanzionatorie, va ritenuta soddisfatta la punizione escludendo la identità della misura della sanzione irrogata.
Per quanto concerne poi le modalità per ridurre la sanzione detentiva bisognerà ricorrere ai criteri di ragguaglio noti al codice penale, nel rapportare un giorno di detenzione al corrispondente valore economico[15].

5. *Il delitto di trattamento illecito di dati*. La nuova disposizione dell'art. 167 CdP sostituisce integralmente la norma abrogata che, peraltro, non reca con sé neppure problemi applicativi legati alla successione delle leggi penali nel tempo.
La modifica è stata radicale e abbraccia tutti gli elementi costitutivi della fattispecie, in parte correggendo anche talune distorsioni tecniche della vecchia disciplina che ne impediva un'agevole lettura[16].
5.1. *Lineamenti di struttura del fatto*. Va subito notato che, diversamente dalle altre rubriche che titolano i reati che seguono nel provvedimento legislativo, in questa manca la specificazione del carattere di "*personali*" dei dati, lasciando un margine di perplessità sulla mancata precisione legislativa.
L'art. 167 CdP costituisce una disposizione complessa, al cui interno sono riportate tre diverse ipotesi di reato di trattamento illecito di dati personali, ciascuna condizionata nei suoi effetti applicativi dalla clausola di sussidiarietà per impedire il concorso materiale con altri reati analoghi e concorrenti.

---

[15] Seppure vi siano propositi di modificare in aumento l'ammontare del valore economico monetario da ragguagliare al giorno di pena detentiva, attualmente l'art. 135 c.p. "*Ragguaglio fra pene pecuniarie e pene detentive*" stabilisce: "*Quando, per qualsiasi effetto giuridico, si deve eseguire un ragguaglio fra pene pecuniarie e pene detentive, il computo ha luogo calcolando euro 250, o frazione di euro 250, di pena pecuniaria per un giorno di pena detentiva*".

[16] Essa stabilisce: "*1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni. 3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato*".

Il legislatore non si è discostato con l'attuale riforma dal precedente modello di incriminazione che vedeva il disvalore di questa ipotesi subordinato all'eventuale applicazione di una fattispecie incriminatrice più grave. L'esordio, infatti, di tutte e tre le ipotesi è con l'*incipit* "*Salvo che il fatto non costituisca più grave reato*" ponendo in ombra l'oggettiva rilevanza autonoma di queste condotte offensive che invece vengono assorbite in una fattispecie diversa, più grave sul piano della misura della sanzione e sostanzialmente differente per la categoria giuridica di appartenenza dell'illecito.

Mai come in questo caso andrebbe rivisto il principio di sussidiarietà in punto di gravità, poiché la legislazione ancora non scioglie il nodo problematico circa la differenza tra il giudizio di gravità in astratto e quello di gravità in concreto. L'attuale assetto sanzionatorio del catalogo appartenente all'attuale legislazione penale, dopo aver introdotto pene patrimoniali e valorizzato tutto il complesso quadro di sanzioni collaterali, come ad esempio, la confisca quale misura di sicurezza nella nuova formulazione dell'art. 240 c.p., pone all'interprete un importante dilemma: se non sia più corretto individuare la gravità del reato alla luce di tutto il compendio sanzionatorio, seguendo anche l'impostazione della giurisprudenza convenzionale, ovvero soltanto la pena edittale stabilita per la singola figura di reato.

Nel caso del provvedimento legislativo al nostro esame il tema della gravità è ulteriormente caricato di dubbi, poichè risulta anche contaminato dagli effetti della sovrapposizione tra sanzione penale e sanzione amministrativa. Da qui una netta scissione tra pena in astratto, particolarmente pesante, e pena in concreto molto più contenuta perchè depurata dagli effetti del *ne bis in idem*.

La vera importante novità che si registra è quella che la nuova legge ha riformulato il requisito del nocumento da condizione obiettiva di punibilità a evento del reato per tutte e tre le ipotesi punite dall'art. 167 CdP.

Si tratta di una rilevante differenza, più volte auspicata in dottrina, poichè non si presenta soltanto come soluzione più aderente a principi di correttezza tecnica nella redazione della fattispecie, ma soprattutto come un deciso potenziamento effettivo del disvalore del fatto e della sua concreta applicazione.

Con questa attuale versione della norma si potrà ipotizzare il tentativo di trattamento illecito, fatto che non era possibile ritenere configurabile in assenza di un evento materiale, come l'attuale, nocumento e in presenza di un reato di pericolo. La norma passa dalla natura di reato di pericolo concreto, infatti, in reato con evento di danno con una fase di accertamento dell'evento materiale resa più agevole.

Questa doverosa calibratura degli elementi costitutivi del fatto pone anche in un diverso rapporto il danno, qualificato dal dolo specifico, e il nocumento come evento del delitto.
Nella vecchia disciplina, pur appartenendo il nocumento alla struttura della fattispecie quale condizione obiettiva di punibilità intrinseca, danno e nocumento qualificavano in termini esclusivamente economici il fatto incriminato, sebbene i due elementi fossero indirizzati a obiettivi ben diversi. Il primo rendeva *rilevante* il fatto, il secondo rendeva *punibile* il fatto. Nella fattispecie abrogata, infatti, il nocumento gestiva soltanto un ruolo di punibilità del reato, mentre in quella attuale il nocumento partecipa al giudizio di disvalore e di offensività della fattispecie.
Nella sua nuova qualità di evento il nocumento consente di controllare la gravità del reato, allineando la pena, ai sensi dell'art. 133 c.p., alla oggettiva lesività sociale della condotta tenuta dal colpevole.
Aver trasferito la nuova figura di delitto nella categoria dei reati con evento di danno è peraltro importante anche per il giudizio di colpevolezza del responsabile della violazione, soprattutto in tema di prevedibilità della condanna, secondo quanto disposto dal sistema di punibilità convenzionale europeo dell'art. 6 CEDU.
Non bisogna trascurate che l'attuale Codice del trattamento dei dati personali e il Regolamento europeo, entrato parimenti in vigore nel 2018 in Italia[17], sono informati in maniera molto più incisiva ai parametri europei e soprattutto al diritto giurisprudenziale che costituisce un nuovo formante normativo oltre la legislazione[18].
Piuttosto è importante a questo punto capire se la diversa collocazione del nocumento possa giocare un ruolo diverso sulla prassi giurisprudenziale, per vero modesta in materia, che finora è maturata nella giurisprudenza italiana.
La diversità di fondo, dato acquisito alla dommatica penale, è che se inquadrato come evento, il fatto commesso è già reato consumato; se invece come condizione di punibilità, il fatto ancora non assume alcuna connotazione di illiceità penale e potrebbe rimanere semplicemente una ipotesi di illecito amministrativo o dare luogo al risarcimento dei danni in sede civile. Da qui anche una sensibile differenza circa il ricorso a iniziative cautelari, come il

[17] AA.VV., *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di Finocchiaro G., Bologna, 2017.
[18] ELIA, *Il potere creativo delle Corti costituzionali*, in *La sentenza in Europa, modello, tecnica, stile*, Padova, 1988.

sequestro, che scatta solo in presenza di un reato, per impedirne la reiterazione o l'aggravarsi delle conseguenze dannose di quello già commesso.
Tuttavia, che sia condizione obiettiva o evento, resta il fatto che oggettivamente deve poter costituire una concreta e materiale lesione che dia luogo, indifferentemente, a riduzione del patrimonio o anche a un tipo di compromissione irrimediabile di diversa natura, come quella di carattere morale o sociale.
In realtà, la differenza viene ad emergere su altri profili di complessiva rilevanza dell'illecito penale, vale a dire sul piano della configurabilità di un tentativo mancato e dell'incidenza dell'elemento volitivo sull'evento, in quanto il nocumento considerato quale condizione obiettiva sfuggiva alla consumazione così come sfuggiva all'incidenza del dolo, rimanendo l'elemento soggettivo del fatto legato limitatamente agli altri requisiti di tipicità.
Occorre anche aggiungere che la diversa portata normativa del nocumento assume un significato specifico sulla scelta di politica criminale seguita dal legislatore italiano, avendo rafforzato in questo modo la potenzialità incriminatrice della fattispecie secondo la direttrice: proporzione mezzo punitivo - fine di salvaguardia. Un tale indirizzo è contenuto nello stesso Regolamento comunitario che all'art. 15 consente al legislatore nazionale di introdurre "altre sanzioni", tenendo conto della oggettiva necessità di tutela.
Si tratta di una finalità punitiva complementare che la legge sceglie di seguire, ritenendo insufficiente la tutela assicurata soltanto con la sanzione di natura amministrativa, e seguendo il modello di rafforzamento della protezione in un settore normativo dove sussiste un alto rischio lesivo.

5.2. *Le ipotesi punibili*. La prima fattispecie prevista al primo comma dell'art. 167 CdP punisce con la reclusione da sei mesi a un anno e sei mesi chi viola: l'art. 123 CdP "*Dati relativi al traffico*", ossia il fornitore di servizi di comunicazione che non cancella o che tratta oltre il limite stabilito dati personali (*data retention*)[19]; l'art. 126 CdP "*Dati relativi all'ubicazione*", ossia il fornitore dei servizi di comunicazione che tratta, oltre ai dati di traffico, i dati relativi all'ubicazione dell'utenza; l'art. 130 CdP "*Comunicazioni indesiderate*", ossia chi detiene dati personali e contatta con sistemi automatizzati il pubblico; l'art. 129 CdP "*Elenchi dei contraenti*", chi non osserva i provvedimenti con

[19] FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine*?, in *Dir.pen.cont. - Riv.trim.*, 2014, fasc. 2, 178.

cui il Garante fissa modalità e tempi di inserimento di dati personali negli elenchi pubblici dei consumatori per l'invio di materiale pubblicitario.
La fattispecie del secondo comma dell'art. 167 CdP punisce con la reclusione da uno a tre anni chi viola l'art. 9 del Regolamento europeo "*Trattamento di categorie particolari di dati personali*", ossia chi tratta dati personalissimi, come le opinioni politiche religiose etc., dati biometrici e dati genetici, salvo che non sia stato reso un consenso esplicito; l'art. 10 del Regolamento europeo "*Trattamento dei dati relativi a condanne penali e reati*", relativi a procedimenti penali esauriti o ancora in corso (richiamando indirettamente il nuovo art. 2-*sexies* CdP) e gli archivi che detengono documenti o dati di carattere amministrativo o sanitario.
La figura di reato del terzo comma dell'art. 167 CdP, infine, punisce con la reclusione da uno a tre anni chi trasferisce dati personali verso un paese terzo o un'organizzazione internazionale violando l'art. 45 del Regolamento europeo "*Trasferimento sulla base di una decisione di adeguatezza*", solo se la Commissione ha verificato un livello di protezione adeguata dei dati presso il destinatario; l'art. 46 del Regolamento europeo "*Trasferimento soggetto a garanzie adeguate*", se in assenza di una previa verifica il destinatario garantisca un livello di garanzie adeguato e strumenti per azionare i diritti; l'art. 49 del Regolamento europeo "*Deroghe in specifiche situazioni*", nei casi di attività di impresa, l'interessato abbia prestato il consenso o i dati devono essere trasmessi inderogabilmente o per necessità.
Ancora una volta l'impianto complessivo del settore delle norme penali, enormemente lievitato rispetto al precedente Codice, risulta pesantemente caratterizzato da rinvii di tipo recettizio ad altre norme dello stesso Codice e di altri testi[20]. Anche in questo caso se la contemporanea presenza delle norme rinviate non apre apparentemente il *vulnus* al principio di riserva di legge relativa, facendo ricorso alla tecnica della norma penale in bianco, lascia mol-

[20] Corte cost., n. 282 del 990: "*In ordine alla delimitazione dei rapporti tra legge penale e fonti subordinate alla medesima, è giurisprudenza costante di questa Corte il ritenere che il principio di legalità in materia penale è soddisfatto, sotto il profilo della riserva di legge (art. 25, secondo comma, Cost.) allorquando la legge determina con sufficiente specificazione il fatto cui è riferita la sanzione penale. In corrispondenza della ratio garantista della riserva, è infatti necessario che la legge consenta di distinguere tra la sfera del lecito e quella dell'illecito, fornendo a tal fine un'indicazione normativa sufficiente ad orientare la condotta dei consociati (cfr. sentenza di questa Corte n. 364 del 1988)*"; ed ancora: "*.....l'alternativa sarebbe quella di rimettere al giudice l'interpretazione dell'elemento normativo; ma ciò determinerebbe un significativo scadimento di certezza conseguente alle inevitabili oscillazioni applicative*". Ampia casistica è proposta anche dalla giurisprudenza di legittimità, come riferito da LUPO, *Cassazione e legalità penale (Convegno Parma, 9-10 ottobre 2015). Relazione introduttiva*, in *Cass. pen.*, 2016, 438. AA.VV., *Cassazione e legalità penale*, a cura di Cadoppi Roma, 2017.

to perplessi i rimandi esistenti all'interno delle norme rinviate a provvedimenti che possono essere assunti in futuro e norme che possono essere introdotte successivamente[21]. Perplessità che si generano in rapporto al principio di colpevolezza e al dettato dell'art. 6 della Convenzione EDU[22].

Questo difetto di legalità viene seppure in parte obliterato o temperato dalla significativa disciplina introdotta con l'art. 2-*ter* "*Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*" del Capo II "Principi" del Codice del trattamento dei dati. La disposizione, per la verità interessante sul piano sistematico, prevede che il trattamento è lecito, secondo quanto disposto dall'art. 6 del Regolamento europeo, soltanto a condizione che sia stato prestato il consenso dell'interessato o quel trattamento sia ritenuto necessario.

Per quanto concerne la fonte che abilita e qualifica tutte le attività di trattamento i legislatori, nazionale ed europeo, hanno dettato un rigoroso principio di riserva di legge: "*La base giuridica prevista dall'art. 6, paragrafo 3 lettera b), del regolamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento*".

Si tratta di una petizione di principio astratta e tipica della *law in the books*, certamente salutare per un sistema che voglia conservare coerenza e assetto esegetico conforme ai principi guida, ma in cui, in realtà, si annida il proposi-

---

[21] Con questo nuovo provvedimento legislativo il legislatore ha marcato in maniera incontrovertibile la funzione sanzionatoria del diritto penale. La scelta di caricare di ulteriore disvalore condotte che sono in parte ricomprese nelle figure degli illeciti amministrativi, mette in evidenza lo spirito repressivo della scelta e, dunque, un uso del diritto penale per dare maggiore peso alla risposta sanzionatoria dell'ordinamento. A partire da PETROCELLI, *Norma penale e regolamento*, in *Scritti giuridici in onore di Alfredo De Marsico*, Milano, 1960, 397; PECORARO ALBANI, *Riserva di legge. Regolamento. Norma penale in bianco*, in *Riv.it.dir. e proc.pen.*, 1959, 762. Sul possibile *vulnus* alla riserva di legge ritorna MAIELLO, *Dommatica e politica criminale nelle interpretazioni in tema di riserva di legge: a proposito di un'ipotesi di depenalizzazione "giurisprudenziale"*, in *questa Rivista,* 1988. CUPELLI, *La legalità delegata. Crisi e attualità della riserva di legge nel diritto penale*, Napoli, 2012. Sul piano generale ancora si rinvia a CUPELLI, *Il problema della legalità penale. Segnali in controtendenza sulla crisi della riserva di legge*, in *Giur. cost.*, 2015, 181.

[22] RIONDATO, *La legalità penale* versus *prevedibilità delle nuove interpretazioni. Novità dal* Corpus Juris *2000*, in *Il* Corpus Juris *2000,* a cura di Picotti. *Nuova formulazione e prospettive di attuazione*, Padova, 2004, 121. VIGANÒ, *Il principio della prevedibilità della decisione giudiziale in materia penale*, in *www.penalecontemporaneo.it*, 19 dicembre 2016. Questione che affonda la sua radice garantista agli albori dell'elaborazione dei principi del diritto penale moderno, come ampiamente trattato da CADOPPI, *Perché il cittadino possa "....esattamente calcolare gl'inconvenienti di un misfatto". Attualità e limiti del pensiero di Beccaria in tema di legalità*, in *L'Indice penale*, 2015, 569.

to di orientare in concreto tutta la disciplina secondo un modello di *law in action*[23].

5.3. *La finalità punitiva.* Non bisogna infatti dimenticare che l'intero assetto della *privacy* deve essere oggi concepita come tutela della persona, il suo agire quotidiano, la sua intimità, oltre a garantire l'integrità della sua personalità o identità informatica nelle complesse dinamiche delle attività economiche e commerciali svolte nello spazio indefinito della Rete[24].
Se ne trova una prima conferma nel Regolamento europeo al Considerando n. 8, anche se il provvedimento poi si apre ad un assetto di protezione molto più ampio che comprende la vita di relazione: "*Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale*".
La tutela, dunque, sembra rivolta a tutte quelle attività che sono suscettibili di valutazione economica, piuttosto che dirette a proteggere il patrimonio morale e personale dell'interessato che diventa operatore nella Rete e, dunque, per questo assume la qualifica giuridica di consumatore[25].
La norma di orientamento sovraordinata di stampo europeo, come si vedrà più avanti, apre tuttavia la discussione su possibili ambivalenze di tutela circa la sua effettiva finalità punitiva. Nelle complesse dinamiche normative del nostro ordinamento giuridico nazionale, infatti, dove si intrecciano diverse ipotesi di reato per i caratteri di interferenza descrittiva, non sembra che il Codice possa essere disapplicato per gli altri innumerevoli casi di lesione dei diritti della persona che a stretto rigore non appartengono al settore commerciale e professionale.
Questo ambito, non è da escludere a priori, anzi si apre anche ad interventi del giudice sovranazionale che sarà chiamato in futuro a dirimere questioni nuove e complesse, con la rapidità che il mercato impone e con gli spazi

[23] CADOPPI, *Il valore del precedente nel diritto penale. Uno studio sulla dimensione* in action *della legalità*, Torino, 1999. PALAZZO, *Legalità fra* law in the books *e* law in action, in *www.penalecontemporaneo.it* in data 13 gennaio 2016. MANES, *Dalla "fattispecie" al "precedente": appunti di "deontologia ermeneutica"*, in *www.penalecontemporaneo.it*.
[24] DE CUPIS, Bilancio di un'esperienza: diritto all'identità personale, in *La lesione dell'identità personale e il danno non patrimoniale*, in *Atti del seminario promosso dal Centro di iniziativa giuridica P. Calamandrei*, Messina, 1982, Milano, 1985. FINOCCHIARO, *Identità personale (voce diritto alla)*, in *Dig. disc. priv.*, Torino, 2010. PINO, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003.
[25] FINOCCHIARO, *Identità personale su internet: il diritto alla contestualizzazione dell'informazione*, in *Dir. dell'inf. e dell'inf.*, n. 3, 2012.

normativi che il Regolamento e il Codice del trattamento dei dati personali consentono[26].

Ma ora veniamo all'analisi dei tre reati che per come appaiono formulati sono esattamente sovrapponibili, soprattutto per la coincidente presenza degli elementi costitutivi che ne delineano il fatto incriminato.

Le norme rinviate aprono una prima divaricazione tra la vecchia e la nuova disciplina dell'art. 167 CdP, in riferimento all'oggetto materiale del reato che si traduce in questa materia nel tipo e nelle modalità del trattamento effettuato.

La norma abrogata, con il primo e il secondo comma, distingueva le ipotesi sulla base della differenza tra dati comuni e dati sensibili (tra cui giudiziari) in maniera molto più netta e definita della versione aggiornata. Oggi il genere di dati che riceve maggiore protezione va sotto la denominazione di "*particolari categorie di dati*".

Nelle ipotesi in vigore, a ben vedere, le tre norme penali coprono un'area di protezione molto più vasta, giungendo a prevedere l'incriminazione, segnatamente con il terzo comma, di condotte di trasferimento transnazionale dei dati personali.

Mentre il carattere dirimente in precedenza era la natura dell'oggetto materiale, vale a dire la categoria di dati, attualmente è il tipo di operazione compiuta che regola la rilevanza del fatto.

L'influenza del Regolamento europeo, peraltro, si avverte molto significativa, anche con lo scopo di conferire omogeneità di disciplina a tutti gli ordinamenti nazionali, secondo il principio di razionalità che deve assistere una legislazione organica multilivello.

Quando si passa a trattare degli altri elementi costitutivi della fattispecie astratta si nota immediatamente che la descrizione della condotta commissiva non muta tra la vecchia e la nuova disciplina, seppure le condotte di trattamento non sono più contenute nello stesso Codice ma nel Regolamento europeo. Non è solo una scelta di opportunità legislativa né di un rinvio recettizio tipico di una norma in bianco, ma di una soluzione di tecnica normativa che tiene conto della disciplina multilivello che impone l'integrazione caso per caso. Ebbene, tutte le norme definitorie che delimitano i concetti e le operazioni,

[26] ARENA, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quad. cost.*, n. 3, 2014. Tra le tante decisioni una particolarmente importante riguarda la calibratura del concetto di trattamento, ritagliato sulla base dell'interpretazione della definizione fornita dalla normativa sovranazionale, in BUSIA, *Le operazioni dei motori di ricerca su internet vanno ricondotte al concetto di "trattamento"*, commento a *Corte di Giustizia dell'unione europea -Grande sezione- 13 maggio 2014 causa C-131/12*, in *Guida al diritto*, n. 24, 2014.

come quelle del trattamento, sono diffusamente indicate e specificate nell'art. 4 "*Definizioni*", posto a rimarcare che nella fase applicativa il giudice dovrà uniformemente sussumere determinati fatti senza lasciare alcuna discrezionalità ai legislatori nazionali, che potrebbero con le loro scelte confondere il quadro di unicità e conformità delle prescrizioni, in ossequio al principio di uguaglianza ed equità.

5.4. *Il soggetto agente e le modalità di trattamento dei dati*. Prima di tutto, spicca la figura del soggetto agente che non viene identificato con una qualifica soggettiva che ne connota la particolare attività professionale, limitandosi il legislatore ad esordire con la locuzione: "chiunque".
Si tratta, dunque, di una generica categoria di soggetti che delinea la fattispecie incriminatrice come reato comune, diversamente da quanto si legge nei percorsi parlamentari in riferimento ad una prima versione della norma.
In realtà, le prime figure ad emergere nella indistinta categoria dell'agente sono il Titolare e il Responsabile del trattamento, che per l'ampia portata *transnazionale* possono operare sia all'interno del territorio europeo sia in territori di Stati esteri.
Su questo tema occorre rinviare alla puntuale definizione normativa fornita dalla disciplina dell'art. 4 del Regolamento europeo, senza escludere, come già detto, che anche persone non rivestite delle stesse qualifiche possano rendersi responsabili del reato.
Sul titolare e sul responsabile grava un impegno di agire sociale tipico della categoria dell'etica pubblica. Infatti, il Regolamento europeo ruota intorno al concetto di "responsabilizzazione" (*accountability*) soprattutto appuntandone l'onere sui due soggetti preposti al trattamento[27].
A ben vedere, per quanto invece concerne il compimento delle attività di trattamento anche altri soggetti che professionalmente svolgono l'attività potrebbero commettere il reato, non limitando la legge la punibilità soltanto al titolare e al responsabile, come peraltro stabilisce lo stesso Regolamento al Considerando n. 9, in cui viene espressamente previsto che: "*Il titolare del trattamento che effettua il trattamento dei dati personali dovrebbe indicare le persone autorizzate all'interno dello stesso titolare del trattamento*".
Il principio di carattere generale che connota le modalità con cui vengono effettuate le operazioni di trattamento resta quello stabilito al Considerando n. 39.

[27] Anche questa è categoria rivisitata dalla modernità, come in JONAS, *Il principio responsabilità. Un'etica per la civiltà tecnologica,* Torino, 2006.

In ordine, invece, al principio generale che consente di trattare i dati personali sono fissati due presupposti fondamentali con il Considerando n. 40.

5.5. Il trattamento contro la sfera personale dell'interessato anche come pretesa di tutela della riservatezza. La scelta di configurare, *ex parte attiva*, un soggetto non rivestito da una specifica qualifica soggettiva, apre la strada alla possibilità che questo delitto possa essere commesso da un soggetto non professionalmente investito di compiti istituzionali di trattamento[28].

Per cui, colui che procede al trattamento potrebbe essere anche un qualsiasi privato che commette questo reato in Rete anche in forma episodica e al di fuori di una struttura organizzata, un singolo tuttavia che sia animato dalla volontà colpevole di produrre nocumento per esclusiva finalità di danno a terzi ben individuabili, per ragioni che prescindono da questioni di carattere commerciale ed economico.

Vi è specifica traccia nei lavori preparatori parlamentari, anche se occorre verificare se la scelta in questo senso è stata adeguatamente orientata nell'ambito della soluzione normativa adottata[29].

Altro aspetto che non può sfuggire è che la descrizione del precetto, pur essendo molto simile a quella abrogata, presenta in una diversa collocazione il requisito dell'evento e, dunque, anche del livello di lesività materiale derivante dalla nuova opzione di politica criminale, nonché l'eliminazione del trattamento che si sostanzia nella comunicazione o diffusione dei dati personali[30].

---

[28] Interessante è anche l'ipotesi di trattamento illecito di dati personali lecitamente posseduti che coinvolgeva la vecchia fattispecie e continua ad interessare l'attuale, nello specifico dell'ipotesi si veda TRIB. MILANO, 8 novembre 2006, in *Giur. merito*, con nota di Pioletti, 2012, 9, 1936.

[29] In particolare, si fa riferimento all'Audizione di Antonello Soro, Presidente del Garante per la protezione dei dati personali, sull'Atto del Governo n. 22 "*Adeguamento normativa nazionale circa la protezione delle persone fisiche con riguardo al trattamento dei dati personali*" presso Commissioni speciali su atti urgenti del Governo congiunte Senato e Camera in data 7 giugno 2018: "*In ordine alle fattispecie penali, pur nella consapevolezza dell'esigenza di evitate ogni possibile violazione del ne bis in idem, abbiamo ritenuto rischiosa la soppressione delle ipotesi di trattamento illecito di dati personali sorrette da fini di danno e non di mero profitto (si pensi al caso di Tiziana Cantone, al revenge porn ecc.), in quanto espressive di un disvalore non minore (anzi generalmente maggiore) delle seconde*", in *www.garanteprivacy.it*.

[30] Il precedente art. 167 CdP titolava "*Trattamento illecito di dati*", infatti, prevedeva: "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".

L'indicazione del profitto e del danno, inteso dal legislatore europeo in chiave economica, come unica finalità ulteriore assegnata all'elemento soggettivo del fatto nella forma del dolo specifico, potrebbe fare escludere che questa norma costituisca un presidio di tutela per vicende di natura personale. Effettivamente l'attuale sfondo su cui si muove la piattaforma normativa penalistica sembra essere quella di stampo economico-patrimoniale, quella stessa che ha animato il movente legislativo di regolazione e tutela del mercato.
A stretto rigore non sembra che nelle premesse legislative si trovi spazio e ragione per circostanze, seppure acquisite e veicolate in Rete senza il consenso dell'interessato che riguardano la vita privata e addirittura intima degli interessati.
Ma occorre fare una doverosa precisazione, poiché la fattispecie oggettiva della nuova figura di reato, alla luce di un'attenta e ampia ricognizione normativa, potrebbe essere orientata anche alla copertura parziale dell'area della riservatezza, intesa come uno di quegli aspetti che può essere attinto dalla lesività della Rete attraverso l'uso illecito dei dati personali.
La questione assume una notevolissima rilevanza sociale forse del tutto inaspettata nella prospettiva in cui si muoveva il legislatore sovranazionale in questa materia. L'assunto da cui si parte, del tutto smentito come indirizzo esclusivo, è che la Rete possa convogliare interessi soltanto di natura commerciale, quando invece è comune esperienza che la Rete consente di intessere relazioni personali e addirittura intime del tutto prive di presidi di tutela, ma connotate da altissimo disvalore.
Né il codice penale può aiutare in questi casi, ampliando la base applicativa dei reati, dato il vincolo di determinatezza e il divieto di analogia che non consentono di andare oltre l'interpretazione estensiva[31].
Il mondo di *Internet* deve vivere di regole proprie e di una tutela specifica ed appropriata per una società umana immateriale che non trova alcun referente adattativo in un tessuto legislativo che regola i rapporti e le relazioni del mondo materiale tra gli uomini.

5.5.1. *Il diritto alla riservatezza leso dal profitto per via indiretta.* Pertanto, se è vero che la nuova incriminazione abbraccia sia fatti che si connotano economicamente sia fatti della vita privata che si divulgano attraverso la diffusione

[31] Il caso della diffamazione commessa con l'uso dei blog viene ritenuto, tuttavia, dalla giurisprudenza ipotesi di diffamazione aggravata "con il mezzo della pubblicità" nella impossibilità di assimilare per analogia il mezzo della Rete con la stampa, come confermato da Cass., Sez. V, 22 gennaio 2019, in *www.cassazione.it*.

dei dati identificativi della persona, occorre puntualizzare in quale modo gli ultimi potrebbero ricevere tutela dal delitto di trattamento illecito di dati personali.
Seppure non connotati da valore economico le fotografie e i filmati postati in Rete, che siano di vita comune o di vita intima, senza il consenso degli interessati, in cui la vita privata si traduce in trattamento di dati personali, l'uso che talune piattaforme informatiche potrebbero farne andrebbe a rivelare un insospettabile risvolto di carattere patrimoniale.
Ed infatti, il profitto economico ricavabile dalla diffusione in Rete potrebbe avvenire allorchè un soggetto dovesse essere venuto in possesso del file. In qualità di titolare o di responsabile del trattamento questo operatore economico potrebbe allegarvi inserti pubblicitari destinati a produrre reddito, proprio perchè questi filmati sono in grado di suscitare interesse nel pubblico dei consumatori o dei frequentatori quella piattaforma. Più persone si affacciano a visionare il filmato maggiore è il vantaggio economico che si trarrà per il messaggio pubblicitario che viene diffuso in Rete su quella piattaforma.
In questa prospettiva il requisito di tipicità che immediatamente non si coglie, finisce per diventare rilevante attraverso l'uso di "contenitore" di dati personali, cioè la *clip* inserita che svela l'età dei partecipanti, il luogo privato filmato, l'immagine fisica, le relazioni con altri soggetti presenti e prossimi ma anche assenti, la natura della relazione, la ragione degli incontri, tanto da determinare un sicuro e lucroso vantaggio economico per il sito *Internet* che lo ha postato.
In altre parole, non sarebbe penalmente rilevante quella condotta nell'immediatezza, ma lo potrebbe diventare alla luce delle modalità di utilizzo e di gestione di quei dati personali.
Ecco allora che il profitto, per sé o per altri, o il danno all'interessato in questa specifica ipotesi potrebbero celare un risvolto applicativo del tutto inatteso, anzi viene valorizzata la proposizione disgiuntiva "ovvero" che sgancia proprio il danno dal profitto. Danno e profitto, pur quantificabili nella stessa misura assumono una valenza del tutto diversa ai fini della configurabilità del fatto, anzi ne divaricano la forbice della tipicità. Potrebbe essere sufficiente il profitto per la configurabilità del reato che troverebbe una sua coerente ricaduta nell'evento del nocumento che presenta nella sua ampia accezione connotazioni di natura patrimoniale.
A ben vedere, seppure sagomata sulla finalità esclusivamente patrimoniale, la fattispecie si potrebbe prestare a obiettivi diversi, quella stessa che diventa importante per i contatti e i contratti in Rete per potervi operare nei termini

dell'*e-commerce*, in quanto rese rilevanti soltanto in maniera indiretta rispetto alle originarie intenzioni punitive.

5.5.2. *Il diritto alla riservatezza leso dal danno per via diretta*. Questione del tutto diversa e a questo punto inedita è quella che concerne il trattamento illecito con esclusiva finalità di danno, quando non vi sia alcun fine di profitto diretto o indiretto ma soltanto la volontà finalizzata ad arrecare nocumento di natura sociale e morale.
Prima di tutto si pone un serio problema che investe sia la qualifica del soggetto attivo sia l'area di tutela della riservatezza che, almeno stando ai lavori parlamentari, sembra voler comprendere le nuove figure di reato.
Il Considerando n. 8, di cui sopra si è detto, apre una seria riflessione su questi propositi, poiché, nell'indicare tra i possibili autori "*una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico*" aggiunge in maniera laconica che non è tutelato il trattamento che non abbia "*una connessione con un'attività commerciale o professionale*".
Questa evidente direzione che finalizza il trattamento appare in perfetta sintonia con il fine di profitto contenuto nella norma, ma non perfettamente in linea con un danno che non sia legato a un criterio strettamente economico e commerciale bensì soltanto di natura morale e personale. Si badi che poi la norma penale associa il danno e il nocumento facendo rientrare nel quadro dell'offesa anche lesioni di natura non patrimoniale.
Vi sono state due importanti vicende di cronaca, tra le tante, che depongono in questo senso e che già appartengono alle scelte selettive dell'ordinamento italiano. Il caso che ha visto al centro di un processo penale i responsabili della società *Google Italy Srl*, incriminati per la diffusione di un filmato denominato "*Vividown*"[32] e quello che riguardava i filmati privatissimi di una giovane, purtroppo morta suicida, vittima del c.d. fenomeno del *revenge porn*, il cui procedimento penale ha registrato un decreto di archiviazione degli atti[33].
Questi accadimenti di cronaca propongono, oltre che alla sensibilità del legislatore già ampiamente espressa a favore, all'attenzione dell'interprete una seria e meditata riflessione.

[32] Ci sia consentito rinviare a TRONCONE, *Il caso GOOGLE (e non solo). Il trattamento dei dati personali e i controversi requisiti di rilevanza penale del fatto*, in *Cass. pen.*, 2014, 2060.
[33] Per la rimozione dei filmanti in Rete si rinvia all'esito del procedimento per reclamo a Trib. Napoli-Nord, Ordinanza proc. n. 9799/16 del 3 novembre 2016, in *www.iurisprudentia.it* di accoglimento della richiesta.

Peraltro, mai come in questa materia gli interventi della giurisprudenza normativa sono stati opportuni perché hanno permesso di tarare meglio la norma in termini di concretezza, facendola uscire dal cono d'ombra della simbolicità punitiva. L'ampliamento del quadro di lesività ha fatto in modo da ricomprendervi la tutela di fatti della vita privata delle persone che vanno ben oltre lo stretto significato che esprime un dato personale identificativo seppure di natura comune o sensibile[34].

La nuova disciplina chiama peraltro l'interprete a fare i conti con un'indagine normativa multilivello, attraverso i numerosi rinvii recettizi, per verificare se aspetti della vita sociale che invocano urgenza di protezione possano essere presi in considerazione. Lo sforzo esegetico si impone anche perché la nuova disciplina si pone obiettivi del tutto nuovi e inediti, forse anche per lo stesso legislatore nazionale.

Occorre tenere presente che il delitto dell'art. 167 CdP, rifratto in tre diverse ipotesi, si presenta del tutto diverso dalle precedenti fattispecie. Il precetto è stato da una parte riordinato dei suoi requisiti di tipicità, d'altra parte gli elementi costitutivi di rilevanza del fatto, in particolare la comunicazione e la diffusione, sono transitati nella ipotesi di reato rubricata alla norma successiva[35].

Il versante del danno come finalità dell'elemento del dolo legato agli effetti del nocumento questa volta qualificato come evento consente una ricostru-

---

[34] La giurisprudenza amplia infatti la piattaforma applicativa della disciplina nel suo complesso, facendovi rientrare "*il suo stato di famiglia, il fatto di vivere da sola, la proposizione della domanda di rateizzazione, il mancato accoglimento della stessa*", tutte circostanze che attengono alla vita personale e intima della parte danneggiata, come afferma Cass,. Sez. II civile, Sent. n. 18292 del 17 dicembre 2019, in *www.cassazione.it.*

[35] La scelta di collocare i requisiti di tipicità della comunicazione o della diffusione in una diversa fattispecie giova alla configurabilità del nuovo reato, libero da una serie di passaggi obbligati che lo rendevano di incerta concretezza applicativa, sul punto Cass., Sez. III, 14 giugno 2017 in *www.cassazione.it.*: *".....il trattamento dei dati personali del XXXX, trattamento che comprende la raccolta, la conservazione, l'elaborazione e la comunicazione a terzi delle immagini della p.o., per un fine di profitto e con causazione di un nocumento che non devono necessariamente rivestire natura patrimoniale", è l'accertamento, considerato correttamente necessario dal primo motivo di ricorso, in particolare di una condotta di destinazione alla diffusione o alla comunicazione sistematica senza le quali il trattamento stesso non potrebbe, infatti, ricadere nell'ambito della normativa in oggetto*". Ed ancora, in relazione a quanto previsto dall'art. 5, comma 3, del D.Lgs. n. 196 del 2003: "*.....il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione"; ed al riguardo, precisa poi l'art.4, comma 1, lett. m) dello stesso d.lgs., dedicato alle definizioni, che la diffusione deve intendersi come "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione". Sicchè, in altri termini, affinchè il reato sia integrato, anche nella forma della trasmissione o consegna a soggetti determinati, è necessario che i dati siano comunque destinati ad una diffusione*".

zione del fatto completamente diversa dal passato, ricomprendendovi anche fatti della vita privata di una persona.
Prima di tutto occorre partire dalle norme rinviate contenute nel secondo comma dell'art. 167 CdP e in particolare dalla disciplina dell'art. 2-*sexies* CdP "*Trattamento di categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante*"[36].
Il richiamo all'art 9 del Regolamento europeo è decisivo e mette in evidenza il fatto che deve trattarsi di dati personali, in passato definiti sensibili, ora indicati come appartenenti a categorie particolari. Ed infatti, quando si analizza l'art. 9 "*Trattamento di categorie particolari di dati personali*" si ritrovano aspetti e risvolti che fuoriescono a stretto rigore dalla categoria di dati e integrano invece circostanze di vita privata[37].
Si diceva prima che la giurisprudenza sotto la norma abrogata aveva aperto un deciso varco in proposito, perché aveva valorizzato la connotazione di lesività del nocumento, portando a ritenere la condizione obiettiva di punibilità non estraneo al fatto, ma come un elemento interno alla fattispecie che partecipa alla produzione degli effetti lesivi[38]. A stretto rigore questa lettura avvicina, sia

[36] Esso stabilisce: "*1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonchè le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*".

[37] Dispone la norma: "*1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita asessuale o all'orientamento sessuale della persona. 2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;*".

[38] Sul punto si rivela preziosa l'opera giurisprudenziale di adattamento normativo che la Corte di Cassazione ha compiuto in questi anni, nel riconoscere al reato abrogato una portata certamente più puntuale e aderente ai principi generali del diritto penale. Il requisito del nocumento, indipendentemente dalla sua qualificazione in termini di condizione obiettiva di punibilità ovvero di elemento costitutivo del reato, in concreto deve essere inteso come un pregiudizio giuridicamente rilevante di qualsiasi natura, patrimoniale o non patrimoniale, subìto dalla persona alla quale si riferiscono i dati o le informazioni protetti dalla legge, come afferma Cass., Sez. III, 14 giugno 2017 *cit.*: "*Alla luce di tale inquadramento, ben può dunque rientrare, nel concetto di nocumento, nella specie in particolare non patrimoniale, come ritenuto dalla sentenza impugnata, la forte preoccupazione per la propria incolumità e per i propri beni derivante dalla comunicazione di dati personali a soggetti sconosciuti in un contesto connotato dal rinvenimento, unitamente alle immagini stese, di un dossier comprendente informazioni sulla propria vettura, già in precedenza oggetto di danneggiamento, e della fotografia di casa con contrassegnati i vari punti di accesso.*"

nel suo significato intrinseco che nella funzione politico criminale, la condizione obiettiva all'evento, distinguendone il carattere qualificativo solo per la copertura dell'elemento soggettivo[39].
Tutto ciò diventava possibile per il fatto che la norma ricomprendeva nella stessa orbita di lesività, sempre nella direzione del dolo specifico, il danno, ma avendo anche presente che il nocumento non è altro che un segmento costitutivo nel concetto di nocumento, in una sorta di duplicazione o rafforzamento del carattere di concreta offensività.
Passando ora a considerare quali sono i risultati di un'indagine sistematica condotta sull'intera legislazione penale, emerge in maniera incontrovertibile che il settore dei reati informatici presentano una fattispecie incriminatrice non troppo distante da quella in esame[40]. Il caso in riferimento è quella descritta dall'art. 617-*septies* c.p. "*Diffusione di riprese e registrazioni fraudolente*" inserito dal D.Lgs. n. 216 del 29 dicembre 2017. In questa ipotesi di reato emerge con chiarezza che a limitare gli effetti della norma soccorre una descrizione che declina la punibilità unicamente all'offesa prodotta alla reputazione o all'immagine.
La portata offensiva del paradigma punitivo è certamente interessante perché in parte viene recuperato il valore della reputazione appartenente in precedenza al delitto di diffamazione, che oggi vede riabilitata la possibilità di concretizzazione con condotte che vengono compiute attraverso la frode.
Nelle intenzioni del legislatore sicuramente si agitavano finalità di tutela del principio della segretezza delle comunicazioni come vuole l'art. 15 della Costituzione e come del resto appartiene alla stessa categoria teleologica il contesto legislativo del trattamento dei dati.
L'indagine sugli elementi costitutivi del reato spinge anche a qualificare questa ipotesi in rapporto di *species* a *genus* con il delitto, in gran parte confinato alla storia della legislazione italiana, di diffamazione. Questo tipo di interferenza normativa che mette in evidenza una parziale identità del fatto incriminato in astratto diventa materia di accertamento per individuare quale sia la

[39] Ci sia ancora una volta consentito di rinviare alla questione specificamente trattata in TRONCONE, *Il delitto di trattamento illecito di dati personali*, Torino, 2011, 157; nella nuova prospettiva descrittiva si rinvia a TRONCONE, *La tutela penale della riservatezza e dei dati personali. Profili dommatici e nuovi approdi normativi*, Napoli, 2020, 117.
[40] Si tratta del prodotto generato dall'onda lunga della ratifica della *Convenzione di Budapest* del 23 novembre 2001, in AA.VV., *Le nuove leggi penali. Sistema penale e criminalità informatica*, a cura di Luparia, Milano, 2009. COLOMBO, *La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali*, in *Ciber. e dir.*, vol. 10, n. 3-4, 2009. Per un precedente inquadramento normativo, si rinvia a PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999.

norma prevalente da applicare alla fattispecie concreta attesa la presenza della clausola di sussidiarietà.
Ebbene occorre concludere che rispetto ad una fattispecie concreta che sembra apparentemente rientrare nella descrizione sia dall'art. 167 CdP, II comma, che dall'art. 617-*septies* c.p. finisce sempre per prevalere la seconda ipotesi di reato, in considerazione del fatto che la pena, e dunque la gravità in astratto, è della reclusione fino a quattro anni, ben maggiore rispetto alla pena della reclusione da uno a tre anni del delitto di trattamento illecito di dati personali.
Naturalmente l'elemento divaricatore e, dunque, il discrimine applicativo, è costituito dall'elemento specializzante della frode captativa che risolve in radice l'eventuale conflitto apparente di norme.
Quando invece viene manifestato il consenso dalla vittima e la sua partecipazione consapevole ad essere ripresa in circostanze intime, la diffusione di quelle immagini o delle conversazioni fa sorgere la questione in termini di concorso di reati e la necessità di verificare gli effetti della prevalenza applicativa a favore dell'illecito trattamento di dati.

5.6. *La categoria del soggetto passivo e il dato personale a carattere identificativo.* Molto interessante è il fatto, probabilmente sfuggito anche in sede di riformulazione della norma, che sia il danno che il nocumento oggi si presentano in maniera soggettivamente qualificata, mentre in passato erano privi di una esplicita relazione con posizioni giuridiche soggettive. La vera novità è che la vigente disciplina declina, in tutte e tre le ipotesi di reato, in termini personali il reato, fondandone la *ratio* sulla posizione giuridica soggettiva dell'interessato a tutela dei suoi diritti o dei suoi legittimi interessi[41]. Tra l'altro la categoria dell'interessato raccoglie oggi anche la figura del soggetto minore di età che abbia però più di sedici anni, senza escludere che la frequentazione in Rete avviene anche da parte di adolescenti che scambiano e diffondo, nell'inconsapevolezza dei rischi, i propri dati personali.
Questa esplicita indicazione del referente soggettivo aiuta anche a definire meglio la categoria del soggetto passivo appartenente alla fattispecie oggettiva del fatto.
Il vecchio art. 167 CdP non indicava in nessuno dei due commi, si legga reato, chi fosse il soggetto cui era rivolta la condotta offensiva punibile. Oggi con l'indicazione esplicita della qualifica soggettiva di interessato possiamo age-

[41] LO SURDO, *Dati personali e strumenti di tutela del soggetto "interessato"*, in *Danno e responsabilità*, n. 2, 2003.

volmente individuare la categoria del danneggiato, abilitato a costituirsi parte civile nel processo penale: colui e soltanto colui che ha subito il nocumento. La vecchia formulazione si prestava in realtà ad una equivoca interpretazione, poiché legava il soggetto passivo indeterminato e indeterminabile alla verificazione della condizione obiettiva di punibilità, lasciando nel vago la individuazione mirata e certa della posizione giuridica su cui si era determinato il danno.
Aver legato oggi il soggetto passivo qualificato all'evento vuol dire offrire oggi al giudice uno strumento di accertamento calibrato per ricercare su quella specifica e circoscritta posizione giuridica soggettiva se il nocumento si sia materializzato e in quale misura per consentire poi la successiva quantificazione della pena da applicare al colpevole.
Questa soluzione sembra adeguata anche a risolvere il problema della colpevolezza del soggetto agente, poichè la scelta normativa, svolgendo una precisa funzione selettiva delle condotte punibili e degli eventi verificatisi, pone in diretta relazione la volontà consapevole e colpevole dell'agente con il soggetto passivo del reato, per rendere ancora più sicura la prova della responsabilità e più qualificata la sua colpevolezza.
Non va dimenticato che questi requisiti di fatto assumono una precisa connotazione processuale sul piano delle garanzie convenzionali, soprattutto per quanto riguarda, come già si è detto, i requisiti di accessibilità e di prevedibilità sanciti all'art 6 della CEDU.
In definitiva, per consentire una corretta opera di sussunzione il legislatore europeo dispiega un catalogo preciso di circostanze, delineando anche la figura dell'interessato con il n. 1) dell'art. 4 del Regolamento europeo: "*1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;*".

5.7. *La nuova previsione dell'evento e i rapporti con il dolo specifico. Evento e tentativo.* Sempre in ordine alla fattispecie oggettiva, in ultimo va inquadrato l'evento e la sua portata innovativa rispetto al passato in cui il nocumento era qualificato dalla stessa norma come condizione obiettiva di punibilità seppure intrinseca al fatto incriminato.

È nota la *querelle* sulla natura della condizione obiettiva tra intrinseca ed estrinseca che mai come nell'ipotesi della formulazione abrogata prendeva concretamente parte al profilo di lesività del reato[42]. Sicuramente le obiezioni sollevate erano fondate per l'ambiguità che il requisito di configurabilità del reato suscitava da un punto di vista tecnico.
In realtà, le perplessità venivano anche destate dal rango di rilevanza penale del fatto che rimaneva, in assenza del verificarsi della condizione, un fatto concreto del tutto indifferente per il diritto penale, nonostante una chiara ed evidente portata offensiva che ne connotava la struttura oggettiva e soggettiva.
Con la nuova disposizione muta soltanto il presupposto della colpevolezza dell'agente, null'altro. Arrecare nocumento all'interessato è la conseguenza della condotta tenuta dal colpevole, causalmente legata al trattamento illecito previsto dalle norme rinviate.
Si tratta di un evento che si concretizza a titolo di dolo generico, attraverso un comportamento rimproverabile perchè consapevole e colpevole. Tuttavia, la volontà di tenere una condotta che si materializzerà in un previsto e voluto nocumento nasce da una condotta commissiva caratterizzata da dolo specifico, diretto ad un evento ulteriore che si concreta in profitto o danno.
Questo è il nodo inestricabile che oggi si presenta all'interprete dal momento che il legislatore non ha voluto sciogliere in maniera tecnicamente più adeguata il legame di disvalore che vede il sovrapporsi del danno al nocumento. Si è già detto che il contenuto di valore è assolutamente identico, semprechè la proposizione disgiuntiva cada a vantaggio del danno e a discapito del profitto - proprio o altrui-, ma la funzione che connota il danno è del tutto diversa da quella posta a presidio del nocumento.
In questo caso il nocumento è certamente coperto dall'elemento soggettivo del fatto, diversamente dalla condizione obiettiva di punibilità che sfuggiva alla volontà, ma la funzione normativa che svolge il danno è del tutto diversa e anzi minaccia l'utilità dell'inquadramento del nocumento come evento del reato.
A stabilire il discrimine di efficacia dell'uno dall'altro è proprio la funzione del requisito soggettivo del dolo specifico che, limitando l'area di punibilità

[42] RAMACCI, *Le condizioni obiettive di punibilità*, Napoli, 1971, 46. NEPPI MODONA, *Concezione realistica del reato e condizioni obiettive di punibilità*, in *Riv. it. dir e proc. pen.*, 1971, 234 e ss. DONINI, *Condizioni obiettive di punibilità*, in *Studium iuris*, 1997, 592 e ss. NEPPI MODONA, *Condizioni obiettive di punibilità*, in *Enc. giur. Treccani*, Roma, 1998, 1 e ss. D'ASCOLA, *Reato e pena nell'analisi delle condizioni obiettive di punibilità*, Napoli, 2004. MASARONE, *Contributo ad uno studio sulle condizioni obiettive di punibilità*, Napoli, 2018.

dei tre reati, riduce anche la portata offensiva dell'evento. In altri termini, soltanto se vi è la prova della fondatezza dell'elemento doloso qualificato dall'evento ulteriore, nella sussistenza del dolo specifico, si passerà a valutare il verificarsi dell'evento o del tentativo compiuto, altrimenti non vi è materia di tipicità.
In questa materia l'elemento soggettivo gioca un ruolo dirimente che va ben oltre il suo stretto ambito di competenza, fino rendersi essenziale per il verificarsi della fattispecie oggettiva del fatto tipico.
Nulla esclude, naturalmente, che quello stesso fatto non punibile per il diritto penale possa rientrare, e certamente vi rientra, nell'area di punibilità dell'illecito amministrativo o possa dare fondamento a una richiesta di risarcimento dei danni per il diritto civile.

5.8. *L'auspicio di una formulazione alternativa.* La norma, o meglio le norme, potevano essere formulate in maniera diversa conferendo la giusta collocazione ai diversi elementi costitutivi del reato, tenuto conto del fatto che il legislatore italiano aveva ricevuto un mandato vincolante dal legislatore sovranazionale. Il precetto poteva corrispondere al seguente testo: "*Salvo che il fatto costituisca più grave reato, chiunque procedendo al trattamento di dati personali in violazione dell'art..... arreca nocumento, è punito con la reclusione....*".
Questa diversa descrizione del precetto avrebbe salvato le norme dal limite di applicabilità pur in presenza di una significativa lesività, però non punibile, a causa della presenza del dolo specifico. Inoltre, sarebbe stata in linea con il dettato dell'art. 13 della legge di delegazione europea n. 163 del 2017 dove è stabilito che la previsione di sanzioni penali doveva essere indirizzata in termini di efficaci, dissuasive e proporzionate alla gravità della violazione.
A questo punto è lecito chiedersi se il legislatore ha mancato il suo obiettivo oppure intendeva impedire che queste norme andassero a punire fatti diversi dal trattamento dei dati personali, vale a dire la sfera della riservatezza personale giungendo a coprire l'area di tutela della dignità personale.
Interrogativo cui è difficile fornire una risposta, se non ricordando che il Regolamento e il Codice del trattamento dei dati personali in origine sembravano posti a tutela delle sole operazioni di mercato, dunque finalità esclusivamente di tipo economico, ben distanti da quelle auspicabili iniziative di tutela del patrimonio morale dell'interessato che lo stesso legislatore italiano, forse pentendosi, aveva dequotato nel loro disvalore penale attraverso la depenalizzazione dei delitti di ingiuria e diffamazione.

Va in ultimo aggiunto che un paracadute di tutela l'interessato lo ritrova nell'ampio corredo dell'illecito amministrativo di cui è dotata la legge, per cui non è del tutto sfornito di difesa. Manca invece quel carattere dissuasivo che è proprio della sanzione penale che attraverso lo stigma che produce potenzia l'efficacia della punizione rispetto a una sanzione pecuniaria di rango amministrativo.

6. *Il delitto di comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala.* La disposizione dell'art. 167-*bis* CdP è la prima delle novità della riforma del Codice del trattamento di dati[43].
La norma sembra si muova su due diverse direttrici che configurano due diverse ipotesi di reato, seppure accomunate dall'unicità dell'oggetto materiale del fatto, vale a dire la comunicazione o la diffusione di un archivio automatizzato o una parte sostanziale di esso.
La vera differenza tra le due fattispecie è data dal requisito di tipicità previsto dal secondo comma e costituito dal mancato consenso dell'interessato.
Proprio alla luce di questo dato di tipicità del fatto è possibile affermare che la vera norma penale, vale a dire quella che nella fisiologia delle connotazioni teoriche di una norma di questo settore possiede le componenti del precetto e della sanzione nonchè una descrizione precisa dei requisiti costitutivi, è soltanto quella rubricata al primo comma.
L'ipotesi di reato del secondo comma invece si limita semplicemente a punire chi esegue il trattamento dati senza richiedere il previo consenso.
La scelta di introdurre una doppia figura di reato, seppure distinta dal requisito del consenso, può essere salutata con favore in una vasta legislazione con alto valore selettivo, perché l'autonomia della fattispecie serve a mettere in risalto l'autonomia dei suoi requisiti costitutivi, secondo il principio di governo della specialità che ne segna la prevalenza rispetto alla fattispecie base dell'art. 167 CdP.
Anche in questo caso si replica la scelta della categoria del soggetto agente che amplia, attraverso la locuzione "chiunque", il novero di coloro che possono

[43] La norma stabilisce: "*1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione*

commettere questi reati. Naturalmente si rinvia a quanto già detto per coloro non qualificati istituzionalmente che non svolgono soltanto attività di trattamento di natura commerciale e professionale sul mercato, come il titolare e il responsabile, ma anche trattamenti di tipo privato o di altra natura.
Uno dei caratteri di tipicità che rende specializzanti le due ipotesi di reato rispetto alla norma punitiva generale è concentrato nel requisito del destinatario del trattamento, dal momento che il legislatore ha inteso indicare come soggetto passivo un'ampia categoria indeterminata, tipica dei reati a soggetto passivo diffuso.
Dall'esame dei lavori preparatori si apprende che la denominazione originaria doveva essere quella del "*rilevante numero di persone*" danneggiate destinatari della comunicazione o diffusione dei dati. Il legislatore delegato ha ripiegato invece su di una indicazione di tipo quantitativo, il "*trattamento su larga scala*", preferendo utilizzare una terminologia tecnicamente più adeguata al settore informatico, piuttosto che affidarsi a un tipo di locuzione definitoria limitata, seppure non nella quantità quanto nella specie.
La differenza non sembra di poco conto, dal momento che si perde la declinazione finalistica sulle "persone", i cui dati vengono utilizzati, per affermare un tipo di indicazione che riguarda la caratteristica, la denominazione, la modalità tecnica del trattamento. Probabilmente la scelta, in un vasto provvedimento che coinvolge una intera comunità di soggetti (o individui, non persone), è apparsa più opportuna perchè sfugge alla genericità e alla indeterminatezza di un elemento costitutivo del fatto.
A ben vedere si sarebbe posta un problema di determinatezza di un elemento qualificativo del fatto, vale a dire il criterio di determinazione del "numero rilevante di persone". Orbene, rispetto a quale parametro quantitativo oggettivo e condiviso assumeva rilevanza l'elemento di configurabilità e poteva diventare punibile il fatto?
Appare evidente, infatti, che riferirsi a una larga scala è una scelta mirata e, in realtà, attinge a un preciso referente normativo generato dal settore tecnologico di appartenenza della norma, cui era opportuno rifarsi per garantire coerenza giuridica alla prescrizione.
Una prima indicazione di orientamento in questo senso la ritroviamo del Considerando n. 6 del Regolamento europeo: "*Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano*" e poi al Considerando n. 91.

Le premesse contenute nei due Considerando, infatti, trovano una puntuale ricaduta nelle norme prescrittive successive stabilite dal Regolamento europeo.
Il riferimento al trattamento su larga scala, la sua spiegazione normativa e tassativa di cosa si voglia intendere con questa espressione, la si ritrova, infatti, all'art. 9 "*Trattamento di categorie particolari di dati personali*" e poi all'art. 10 "*Trattamento dei dati personali relativi a condanne penali e reati*", disposizioni in cui sono indicati i trattamenti per una molteplicità di fini e una generalità indistinta di persone.

6.1. *La condotta punibile*. La condotta punita dalle due ipotesi di reato è identica ed è costituita dalla comunicazione o dalla diffusione di un archivio informatizzato o parte di esso. Essa si connota come condotta commissiva istantanea.
Anche in questo caso la condotta coincide con la forma di trattamento e le diverse forme sono puntualmente qualificate dal Regolamento europeo, vale a dire la fonte normativa di livello superiore e parametro legale di uniformità della disciplina generale. Stabilisce, sul punto, l'art. 4 che il trattamento può consistere: "*in qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come.....la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione.....*".
Si tratta evidentemente di un reato a condotta alternativa che limita lo spazio dell'intervento punitivo di natura penale a precise e tipiche attività di trattamento, in linea con il carattere di specialità della norma.
Il legislatore nel novero delle condotte di trattamento possibili, compiutamente definite all'art. 4 del Regolamento sceglie di punire con una severità sanzionatoria di livello superiore la comunicazione e la diffusione. Peraltro, tra le due condotte sussiste una diversità lesiva, in quanto, soprattutto la diffusione dell'archivio, vale a dire la comunicazione a un numero indiscriminato dei dati, è destinato a cagionare un nocumento maggiormente lesivo agli interessati. Un nocumento, peraltro, che si presenta direttamente proporzionale agli effetti determinati da un fattore moltiplicatore rappresentato dalla potenziale moltitudine dei soggetti coinvolti.
Tutto questo si rende possibile per il fatto che le due specifiche operazioni di trattamento dei dati personali vanno opportunamente distinte per qualificare la gravità di ciascuna di esse, anche ai fini della individuazione della misura della pena da applicare.

Comunicare un archivio informatizzato o parte di esso vuol dire trasferire, trasmettere, notificare a un destinatario individuato il suo contenuto. Si tratta di una definizione, se si vuole anche per il suo valore semantico, che riduce la potenzialità lesiva del mezzo comunicativo rapportandola alla singola entità che la riceve.
Del tutto diversa invece è la condotta a forma diffusiva, destinata a una generalità indeterminata, al punto tale che neppure il responsabile del reato riuscirebbe a identificarla. Questa indeterminabile generalità, presente su territorio nazionale e anche internazionale, conferisce una maggiore gravità al reato, perché la diffusione è indominabile da parte dell'agente e la quantificazione dei destinatari risulta impossibile. Occorre comunque precisare che in punto di pena il legislatore ha inteso punire entrambe le ipotesi con la stessa misura della reclusione.
L'ampio orizzonte fissato dalla definizione del Regolamento europeo pecca tuttavia di determinatezza, perché la due definizioni non sono del tutto eterogenee, anzi, nella diffusione è certamente contenuta la comunicazione. La scelta di politica criminale che giustifica l'esistenza di una norma complessa come quella in esame ha imposto al legislatore italiano di prendere una precisa posizione sul punto e non lasciare nel vago un'indagine sistematica che avrebbe indotto a ritenere trattarsi semplicemente di una inutile duplicazione di una concotta commissiva.
Soccorre a questo proposito il Codice del trattamento dei dati che al n. 4 dell'art. 2-*ter*, peraltro richiamato espressamente dal rinvio operato dal delitto del primo comma dell'art. 167-*bis* CdP, delinea le nozioni di comunicazione e diffusione[44].
Le altre due norme richiamate dall'art. 167-*bis* CdP designano due ipotesi di trattamento connotate da naturali caratteristiche amplificative: l'art. 2-*sexies* "*Trattamento di categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante*" e l'art. 2-*octies* "*Principi relativi al trattamento di dati relativi a condanne penali e reati*", quelle stesse che sono richiamate agli artt. 9 e 10 del Regolamento europeo.

[44] "*Si intende per: a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione; b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*".

6.2. *L'oggetto materiale del reato*. L'oggetto materiale tutelato da queste norme è l'archivio che contiene la pluralità di dati che vengono veicolati all'esterno del loro ambiente digitale consueto da una comunicazione o diffusione.
Prima di ogni altra cosa è necessario chiarire che le due possibili modalità di realizzazione del reato concernono la cessione parziale o totale di un archivio che precedentemente era intesa come una delle possibili forme di trattamento. Oggi invece la legge esplicita in maniera adeguata i canoni di specialità di questa norma rispetto ai reati previsti dall'art. 167 CdP, stabilendo una decisa rilevanza punitiva a condotte che concernono trattamenti su larga scala.
Anche in questo caso la definizione di archivio non viene dedotta dalla sistematica della materia ma dall'oggetto materiale designato dalla base legale del Regolamento europeo con l'art. 4 del Regolamento europeo "*Definizioni*": "*«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;*". Invece con l'art. 2 del Regolamento europeo, viene indicato l'"*Ambito di applicazione materiale*": "*1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi*".
Mentre viene escluso con la lettera c) del comma 2 del predetto art. 2: "*Il presente regolamento non si applica ai trattamenti di dati personali: c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;*"[45].
Con questa disposizione si deduce agevolmente che l'archivio oggetto della norma non è una indeterminata e incoerente quantità di dati personali che a volte si rinvengono nelle agende casalinghe o talvolta nelle memorie dei telefoni cellulari, ma una struttura organizzata secondo dei precisi criteri di classificazione e di indicizzazione che seguano anche il carattere tecnologico della informazione ma non per un uso esclusivamente privato.
La norma riporta come oggetto un archivio o una parte sostanziale di esso. In questo caso la particella disgiuntiva rompe il legame tra un insieme in sé compiuto e un insieme costituito da parte dell'archivio, imponendo un coefficiente di individuazione meramente quantitativo, si indica infatti "una parte

[45] CORRIAS LUCENTE, *Il diritto penale dei mezzi di comunicazione di massa*, Padova, 2000, 118.

sostanziale" di esso. Non è ben chiaro, in assenza di una definizione normativa, cosa si voglia intendere con questa espressione.
Probabilmente una versione più attendibile dovrebbe indirizzare verso una definizione che, tenendo conto di una quantità cospicua di dati, possa costituire un sotto-insieme, un mini-archivio, che tuttavia conservi le caratteristiche tipiche dell'archivio originario, vale a dire la sistematicità secondo criteri preordinati e l'omogeneità dei dati.

6.3. *L'elemento soggettivo del reato*. Anche questo reato si consuma con una condotta istantanea messa in atto da "chiunque", soggetti qualificati, quali il titolare o il responsabile, nonchè soggetti che coltivino una finalità ulteriore, quella di trarre profitto per sè o per altri o per arrecare un danno.
Trattandosi di un reato di pura condotta la norma non designa un evento come conseguenza né tantomeno ricorre all'ipotesi di una condizione obiettiva di punibilità.
Mai come in questo caso l'elemento soggettivo del fatto restringe in maniera consistente l'area di punibilità alle vicende legate ai fini commerciali o economici ovvero per cagionare un danno connotato sempre da carattere economico.
Il caso tipico è quella della cessione di un archivio dei dati personali di consumatori per sfruttarlo con contatti telefonici di offerte commerciali di prodotti di consumo. Da qui anche il carattere di petulanza dei continui contatti telefonici e per posta elettronica che nascono dalla ricerca automatica da parte di sistemi automatici di elaborazione delle informazioni che a caso individuano il numero identificativo del soggetto[46].
Si pensi anche alla cessione di una banca dati genetici che venga utilizzata per fini impropri da concorrenti sul mercato per la ricerca di un vaccino contro la pandemia da COVID-19.

6.4. *La nozione e gli effetti del consenso*. Il delitto del secondo comma, punito con la pena significativa della reclusione da uno a sei anni, riguarda tutte le operazioni di trattamento svolte senza il consenso, quando il consenso è indi-

[46] Questione già nota, si veda ATELLI, *Dal diritto ad essere lasciati soli al diritto ad essere lasciati in pace: la prospettiva del danno di petulanza*, in *Riv. crit. dir. priv.*, 1997. Per altro profilo, attinente all'attendibilità della qualità dei prodotti, si veda DI AMATO, *Il danno da informazione economica*, Napoli, 2004.

spensabile perché richiesto tassativamente dalla legge per la comunicazione o diffusione dei dati[47].
Come sempre la sistematica della materia impone che si parta dalla definizione legale che al n. 11 dell'art. 4 del Regolamento europeo passando poi alle modalità e alle forme di prestazione del consenso, vale quanto stabilito dal Considerando n. 32 del Regolamento europeo.
Questa norma penale si segnala, nella sua singolarità, all'attenzione dell'interprete, poiché la sottolineatura del consenso occorre per la considerevole lesività del reato. Bisogna infatti pensare che i trattamenti su larga scala coinvolgono migliaia e talvolta miliardi di informazioni e dati personali, per cui il consenso diventa assolutamente indispensabile per assicurare una corretta comunicazione o diffusione in ambiti territoriali i cui confini fisici non sono in alcun modo controllabili e contenibili.
Quella in esame è l'unica fattispecie dove si trova inserito tra i requisiti di tipicità del precetto il consenso. L'art. 167 CdP abrogato ruotava intorno al consenso, mentre in questa opera di complessiva riforma della parte penalistica solo la norma in esame lo contempla quale requisito di tipicità del fatto.
Tuttavia, la funzione del consenso quale requisito costitutivo non muta all'interno della nuova fattispecie rispetto al passato, non investendo l'antigiuridicità del fatto come causa di giustificazione, ma confermandosi come elemento costitutivo del fatto tipico.

7. *Il delitto di acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*. Una nuova figura di reato è stata introdotta anche con l'art. art. 167-*ter* "*Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*"[48].
Si tratta di una fattispecie del tutto inedita nel panorama dei reati di trattamento illecito, il cui punto di contatto con le altre fattispecie è il requisito dei dati personali. Su questo punto occorre tuttavia essere più precisi.
Questa fattispecie si pone in diretta relazione funzionale con quella del precedente art. 167 CdP, poichè l'oggetto materiale comune descritto dal fatto è rappresentato dall'archivio automatizzato o parte di esso. La vera differenza è che in questo caso si ha una condotta esattamente opposta a quelle preceden-

[47] MANES P., *Il consenso al trattamento di dati personali*, Padova, 2001.
[48] Stabilisce la nuova norma: "*1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione da uno a quattro anni*".

ti, vale a dire di acquisizione e non si cessione. Questa diversa finalità potrebbe, tuttavia, rilevarsi in una struttura a consumazione sequenziale tra i due reati, allorchè chi avesse acquisito l'archivio lo avesse anche ceduto con la comunicazione o la diffusione.
Naturalmente potrebbe anche accadere diversamente e cioè che la condotta di acquisizione resti senza alcun seguito e l'archivio fosse conservato dal suo illegittimo titolare. Resta il fatto che tale schema operativo può trovare attuazione solo se la condotta tenuta si concretizzi con modalità di frode, cioè artifizi e raggiri, non quando sia sottratto, ad esempio, una memoria di un pc contenente un archivio dati.
Va chiarito che a queste condizioni la norma si pone come antefatto punibile alla precedente ipotesi di comunicazione o diffusione, in una naturale relazione prodromica. Seguendo l'esempio precedente, se l'archivio fosse acquisito in modo diverso dalla frode, si tratterebbe di un antefatto non punibile, salvo che non vi sia un diverso reato consumato come il furto.
In realtà, gli elementi specializzanti della norma potrebbero risolvere naturalmente il concorso materiale di reati a favore del reato speciale rispetto a quello comune, se non vi fosse la clausola di sussidiarietà che finisce per penalizzare proprio l'autonomia normativa della fattispecie.
Il legislatore ha inteso, e non si riesce a comprendere per quali ragioni, tenere distinte la due fattispecie che in realtà, considerate parte di uno stesso fatto con elementi antecedenti e susseguenti, avrebbero segnato un più razionale ed evidente disvalore del fatto.
In realtà una norma analoga, seppure non connotata da elementi specializzati come quelli in esame è già contenuta nel codice penale ed è comprensiva del duplice disvalore costituita dalla condotta di acquisizione e di utilizzazione. Si tratta dell'art. 615-*quater* c.p. "*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*", ma a ben vedere anche gli elementi di tipicità dell'art. 640-*ter* c.p. "*Frode informatica*" delinea lo stesso disvalore della condotta.
Essendo punita questa ipotesi con una pena della reclusione più contenuta non fa scattare la clausola di sussidiarietà dell'art. 167-*ter* CdP, per cui questa seconda norma si potrà applicare in concorso con quella dell'art. 167-*bis* CdP se la successiva condotta si connoterà per la comunicazione o la diffusione dei dati illecitamente acquisiti.
La norma replica in realtà il dolo specifico in linea di coerenza con tutta la disciplina in materia, così come, quale reato di pura condotta, anche questa volta deve trattarsi di un trattamento di dati svolto su larga scala.

7.1. *La condotta di acquisizione con mezzi fraudolenti*. L'elemento specializzante di questa fattispecie è la particolare modalità della condotta che costituisce il presupposto di punibilità dell'agente.
In questo ambito del trattamento dei dati personali ci troviamo certamente in un microsistema di parte speciale, ma resta il fatto che la clausola di sussidiarietà pone all'interprete fondate ragioni per scoprire interferenze normative con altre ipotesi di reato che puniscono casi identici o analoghi rimaste estranee all'attenzione del legislatore. E' evidente che la scoperta di norme analoghe spinge a verificare che non si punisca con le regole di un concorso materiale di reati due volte per la stessa identica fattispecie concreta, oltre alle eventuali chiamate in causa di illeciti amministrativi contenuti nella stessa legge.
La condotta descritta nell'ipotesi in esame rende necessaria l'indagine per accertare le condizioni di consumazione del reato, volgendo al centro della ricerca l'opportunità di controllare se la condotta di acquisizione di un archivio.
A questo punto il problema è comprendere cosa si intenda per oggetto materiale della tutela penale, se ha acquisito una sua concretezza, e quali siano la modalità di realizzazione del fatto costituita dai "mezzi fraudolenti", se si tratta di mezzi tecnologici oppure semplicemente di circostanze in cui si induce a cedere con inganno l'archivio automatizzato.
Per quanto concerne il primo quesito relativo all'oggetto materiale dell'offesa la giurisprudenza penale è orientata apertamente a riconoscerne la natura di reato contro il patrimonio. Gli ultimi approdi, infatti, ridisegnano completamente il perimetro del bene materiale su cui cade la condotta colpevole, per cui **un file è qualificabile come cosa mobile**[49].

[49] Cass. Sez. II penale, Sent. n. 11959 del 10 aprile 2020, in *www.cassazione.it* : "*il file pur non potendo essere materialmente percepito dal punto di vista sensoriale, possiede una dimensione fisica costituita dalla grandezza dei dati che lo compongono, come dimostrano l'esistenza di unità di misurazione della capacità di un file di contenere dati e la differente grandezza dei supporti fisici in cui i files possono essere conservati e elaborati*". E per qualificare la condotta di appropriazione afferma: "*va considerata la capacità del file di essere trasferito da un sopporto informatico ad un altro, mantenendo le proprie caratteristiche strutturali, così come la possibilità che lo stesso viaggi attraverso la rete Internet per essere inviato da un sistema o dispositivo ad un altro sistema, a distanze rilevanti, oppure di essere "custodito" in ambienti "virtuali" (corrispondenti ai luoghi fisici in cui gli elaboratori conservano e trattano i dati informatici)*". Nello stesso senso si era espressa in precedenza Cass., Sez. II, 17 luglio 2018, in *www.cassazione.it*. Per ragioni di completezza va rilevato che in un precedente caso dove si valutava l'applicabilità dell'art. 624 c.p. il giudice era giunto alla medesima determinazione in ordine alla natura materiale del file con Cass., Sez. V, 19 febbraio 2015, in *www.cassazione.it*.

Per quanto poi concerne la modalità della condotta tassativamente richiesta dalla norma va subito registrato che, in un quadro sistematico della materia penale, il legislatore nel 2015, intervenuto in materia tributaria per riformare il D.Lgs. n. 74 del 2000, ha introdotto alla lett. g-ter) dell'art. 1 la nozione penalistica: "*per "mezzi fraudolenti" si intendono condotte artificiose attive nonché quelle omissive realizzate in violazione di uno specifico obbligo giuridico, che determinano una falsa rappresentazione della realtà*".
Anche se per altro settore i criteri dell'interpretazione sistematica, secondo termini di coerenza e di uniformità applicativa che non può prescindere dal dato normativo, amplia il fronte e concentra il disvalore della condotta sui mezzi fraudolenti e non più soltanto su l'atto fraudolento.
Il richiamo agli atteggiamenti omissivi in violazione di un obbligo giuridico determina anche un allargamento del novero delle ipotesi che non si limitano unicamente a condotte commissive, sottolineandone peraltro la precisa portata decettiva.
Non sembra necessario ricorrere a soluzione tecnologiche raffinate per ritenere integrato il mezzo fraudolento, basta in realtà anche un semplice stratagemma per farsi cedere l'archivio automatizzato a corroborare l'ipotesi incriminatrice.
In realtà, molto più vicino per contenuto all'ipotesi in esame è quella stabilita come aggravante speciale del delitto di furto prevista al n. 2 dell'art. 625 c.p. "*se il colpevole usa violenza sulle cose o si vale di un qualsiasi mezzo fraudolento;*", in ordine alla quale le Sezioni Unite della Suprema Corte hanno fornito una definizione molto precisa e quantomai in sintonia con il reato di acquisizione fraudolenta di dati personali[50].
Questo tipo di definizione è molto più aderente anche per l'assimilazione del bene giuridico, in fondo l'archivio automatizzato può essere considerato un bene mobile altrui, soprattutto se l'archivio è contenuto in un supporto informatico come una memoria dati. E così come nel furto aggravato l'archivio può essere sottratto facendo appunto ricorso a un mezzo fraudolento.
Questo punto cui siamo giunti diventa dirimente per rilevare le ipotesi di interferenza normativa, poiché l'ipotesi dell'art. 167-*ter* GdP è una mera ipotesi di furto consumato seppure attraverso la frode.

8. *I nuovi delitti di trattamento illecito di dati giudiziari previsti nel D.Lgs. n. 51/2018*. Nonostante l'entrata in vigore del Regolamento europeo e nono-

[50] Cass., Sez. un., 18 luglio 2013, in *www.cassazione.it*.

stante si discutesse nel Parlamento italiano della nuova legislazione sui dati personali, con una scelta sistematica non del tutto improntata a razionalità legislativa entra in vigore il D.Lgs. n. 51 del 18 maggio 2018 come "*Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonchè alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*" e che ha trovato il suo regolamento attuativo nella Circolare del Ministero della Giustizia 31 maggio 2019[51].
La finalità specifica della legge viene chiaramente esposta all'esordio del testo: "*Il presente decreto si applica al trattamento interamente o parzialmente automatizzato di dati personali delle persone fisiche e al trattamento non automatizzato di dati personali delle persone fisiche contenuti in un archivio o ad esso destinati, svolti dalle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica*".
Questo provvedimento assegna una specifica e autonoma disciplina normativa di settore al trattamento dei dati personali, relativa ai soli dati personali e non di altri, che abbia come obiettivo prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, sostituendo le norme previste nei titoli I e II della Parte seconda del Codice del trattamento dei dati personali per il settore giudiziario, tanto nell'ambito civile quanto in quello penale[52].
La scelta di riconoscere uno statuto regolativo autonomo al trattamento dei dati che appartengono al patrimonio informativo del settore giustizia trova il suo movente legislativo nelle esigenze di sicurezza sociale e giudiziaria che le autorità europee hanno sviluppato in questi anni, al fine di controllare, prevenire e reprimere soprattutto fenomeni di terrorismo internazionale[53]. Il tema che si ripropone è quello del bilanciamento degli interessi e dei principi fondamentali in gioco quando le contingenze di fondati ed incombenti rischi

[51] Serie perplessità di acquisizione e conservazione effettivamente si pongono, in GIROTTO, *Il trattamento dei dati biometrici*, in *Il governo del corpo*, in *Trattato di Biodiritto*, diretto da Rodotà e Zatti, Tomo I, Milano, 2011.
[52] BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in *Cybercrime cit.*, pag. 1599.
[53] RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973. RODOMONTE, *Banca dati della Polizia e diritti della persona*, in *Telem. e diritto*, 1986. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015.

per la sicurezza riducono il peso della *privacy* e consentono l'accesso alle informazioni e ai dati da parte degli operatori dei sistemi di comunicazione[54].
Il quadro normativo messo in piedi con disposizioni di diritto penale ad efficacia transnazionale ha ampliato l'orizzonte attuativo, sviluppando una propria direttrice anche per i fatti di criminalità organizzata, in particolare il traffico di sostanze stupefacenti e i fatti legati alla criminalità economica e degli affari[55].
La finalità della disciplina è dichiaratamente rivolta al controllo delle persone e soprattutto al trattamento dei dati e allo scambio delle informazioni in Rete, per colpire in maniera più efficace fenomeni di allarme oggettivo per la sicurezza dei cittadini europei attraverso il sistema Eurojust[56].
Al Capo VI di questo provvedimento legislativo è prevista con il titolo "*Illeciti penali*" la parte punitiva che contiene norme penali, in particolare il delitto contenuto all'art. 43 denominato "*Trattamento illecito di dati*"[57].
Questa duplice fattispecie, a dispetto della riforma sostanziale della parte penale del CdP che sarà emanato dopo qualche mese, si distingue per ripresen-

[54] Sul punto si rinvia a Corte di Giustizia dell'Unione Europea, Sentenza (Grande Sezione) del 21 dicembre 2016, cause riunite C-203/15 e C-698/15, Tele2 Sverige AB e Secretary of State for the Home Department contro Postoch telestyrelsen e Secretary of State for the Home Department.

[55] Esigenza di sicurezza avvertita ormai da decenni, come allo stesso modo sono state sollevate serie perplessità sui confini di ingerenza nella vita personale dei cittadini per garantirla, in origine RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973. PIZZETTI, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in *www.federalismi.it*. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Dir. Inf.*, 2015, 23. BONINI M., *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in *Riv. AIC*, 18 settembre 2016. BARBERIS, *Non c'è sicurezza senza libertà. Il fallimento delle politiche antiterrorismo*, Bologna, 2017.

[56] "*L'unità di cooperazione Eurojust è stata istituita con decisione 2002/187/GAI del Consiglio modificata dalla decisione 2009/426/GAI del Consiglio, del 16 dicembre 2008. Il compito di Eurojust è essenzialmente quello di potenziare l'efficienza dell'azione delle autorità nazionali impegnate nella lotta contro gravi forme di criminalità organizzata e transnazionale, nell'ottica di favorire un rapido ed efficace perseguimento degli autori dei reati. Eurojust si propone come centro specializzato a livello giudiziario e interlocutore principale nell'adozione di misure efficaci contro la criminalità organizzata transnazionale all'interno dell'Unione europea*", in *www.eurojust.europa.eu*.

[57] La norma stabilisce che: "*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 dall'articolo 5, comma 1, è punito, se dal fatto deriva nocumento, con la reclusione da sei mesi a un anno e sei mesi o, se la condotta comporta comunicazione o diffusione dei dati, con la reclusione da sei mesi a due anni. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sè o per altri profitto o di recare ad un danno, procede al trattamento di dati personali in violazione di quanto disposto dall'articolo 7 o dall'articolo 8, comma 4, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni*".

tare inspiegabilmente una norma esattamente identica a quella dell'art. 167 del Codice del trattamento dei dati abrogata.
Una sorta di recupero di una norma punitiva simbolica priva di efficacia in un assetto normativo che per la sua finalità di tutela sociale esigeva ben altra forma di risposta.
Il profilo dell'imputazione soggettiva è quello consueto in questa materia, al profitto si accompagna il danno che costituisce la finalità ulteriore richiesta per il dolo specifico. Dunque, area di punibilità pesantemente limitata che, unita alle altre restrizioni applicative della norma ne compromette fortemente il profilo di concreta effettività.
Senza ritornare alle note questioni sull'opportunità di introdurre una condizione obiettiva di punibilità, superata nella disciplina generale rinnovata, va precisato che il delitto si configura anche alla sola presenza della comunicazione o della diffusione (come in passato), senza la necessità di valutare il presupposto operativo della condizione.
Intesa in questi termini, con tutti i difetti di una operatività condizionata da elementi costitutivi del fatto inappropriati, questa fattispecie dovrà scontare la sua effettività nella prassi, per comprenderne l'oggettiva potenzialità applicativa.
Già è possibile ipotizzare che la giurisprudenza, sia per l'opera di coerenza sistematica sia per la giurisprudenza consolidata sulla struttura del fatto punibile, si orienterà nel considerare l'evento del delitto quello che immotivatamente è stato inserito come condizione oggettiva di punibilità intrinseca.
Questo provvedimento conserva il pregio di esordire attraverso l'art. 2 "*Definizioni*" con una parte descrittiva che garantisce l'individuazione di condotte e categorie di soggetti operanti e soprattutto conferisce uniformità applicativa.
Importante è la categoria del soggetto agente, determinata con "chiunque", ma designata in definizione con il titolare, il responsabile o l'incaricato del trattamento dei dati personali, esattamente come era stabilito con la disciplina abrogata del precedente art. 167 CdP.

9. *Spunti di diritto processuale penale*. Le tre nuove disposizioni che hanno introdotto le diverse ipotesi di reato trovano un punto di perfetta coincidenza nella disciplina di chiusura degli ultimi commi 4, 5, 6 dell'art. 167 CdP, puntualmente richiamati all'ultimo comma dei successivi artt. 167-*bis* CdP e 167-*ter* CdP che formano l'appendice processuale alla materia di diritto sostanziale.

Si tratta di una scelta strategica del tutto inedita nel panorama della legislazione sostanziale del settore informatico di inserire norme di carattere processuale che investono la fase delle indagini preliminari e, seppure per qualche verso, che investono i presupposti dell'esercizio dell'azione penale.
Nell'epoca di "riserva di codice" la scelta legislativa forse è certamente controcorrente, ma in termini di garanzia e tempestività della prova questo microsistema penale trova proprio nelle norme processuali gli opportuni strumenti attuativi della tutela dei dati personali.
L'art. 167 CdP, richiamato con rinvio recettizio dalle disposizioni penali che seguono, stabilisce che: "*4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante*[58].
Valutando attentamente il dettato operativo espresso dalle norme processuali occorre rilevare che, diversamente dalla scansione delle fasi del processo ordinario, in questo caso le indagini preliminari, ma certamente anche la successiva fase dibattimentale, sono svolte direttamente dall'Ufficio del Garante della *privacy*.
Vi è, infatti, un'opportuna inversione del percorso ordinario. In questo caso è lo stesso Pubblico Ministero a cedere la fase delle indagini preliminari al Garante nella sua qualità di tecnico, con tutta la decisiva attività di raccolta della prova e di adozione di provvedimenti cautelari di natura amministrativa.
Tuttavia, questa nuova veste del Garante non è collocabile nella categoria dei consulenti tecnici, poichè esercita gli stessi poteri del Pubblico Ministero, dando impulso alle indagini e orientando la raccolta del compendio probatorio per profilare la responsabilità del soggetto che ha trattato i dati personali.
In questo modo si realizza invece un vero e proprio trasferimento della funzione e dei poteri di indagine che è tipica dell'ufficio del Pubblico Ministero e della polizia giudiziaria.
La scelta si rivela opportuna perché solo un organo tecnico è in grado di accertare, cogliendo tutti i contorni di una ricerca professionale della prova, i fatti che sono contestati e che risultano connotati da un rilevantissimo profilo di tipo tecnologico. La professionalità in questo caso risolve anche la celerità

[58] La disposizione prevede inoltre: "*5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto. 6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita*".

dei tempi di indagine, evitando di conferire incarichi a tecnici, e realizzando l'aspirazione alla ragionevole durata del processo.
Peraltro, l'attività di raccolta della prova svolta in termini professionali evita anche di coinvolgere nelle indagini persone e soggetti che sono sin dal suo sorgere del tutto estranei, orientando la strategia processuale verso obiettivi attendibili.
Le norme processuali, per conseguire con efficacia l'individuazione dei responsabili e gli elementi di prova utili a sostenere l'accusa nel futuro dibattimento, hanno spinto il legislatore a corredare i poteri ispettivi del Garante di una serie di disposizioni operative che rispondono a criteri di congruità ed efficienza.
Con il precedente Capo III "*Accertamenti e controlli*" del CdP, infatti, è direttamente il legislatore ordinario a conferire specifici poteri di indagine al Garante con gli artt. 157 e 158 CdP.
A queste condizioni, con la raccolta pertinente di elementi necessari a configurare un quadro di indagine processualmente affidabile, spetterà poi al Pubblico Ministero formulare l'accusa e promuovere l'azione penale.
Sul terreno delle norme processuali vi sono altre due disposizioni che destano particolare interesse. Sono inserite in ambiti diversi del Codice del trattamento dei dati, ma convergono verso un unico obiettivo di designare la legittimità di fonti di prova relative ai dati personali. Si tratta del principio di utilizzabilità processuale e del carattere di illegittimità della raccolta della prova che la rende illecita, ovvero ne costituisce il presupposto per una sua sanatoria scanditi dall'art. 2-*decies* CdP "*Inutilizzabilità dei dati*".
Sebbene la nuova legislazione abbia assicurato gli adattamenti necessari alla preesistente normativa penale, il nodo di fondo resta tuttavia ancora, in una società complessa e tecnologicamente onnivora, la necessità di tutelare in termini sempre più stringenti la riservatezza della persona. Riservatezza che, come autonomo bene giuridico di categoria, nella legislazione europea e dei suoi stati nazionali ha trovato ora una solida e riconosciuta base giuridica.
L'esperienza della malattia pandemica da COVID-19 richiama all'attenzione di uno stato democratico, prima di ogni altra cosa, un'ampia convergenza delle diverse fonti del diritto, affinchè in una società dell'immagine e della rapida diffusione delle informazioni la persona umana non resti ostaggio di regole incerte o, peggio ancora, di incolmabili vuoti di tutela, anche quando in gioco sono i più alti valori della giustizia e della legalità.