CJN

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione

IX Corso di formazione interdottorale di Diritto e Procedura penale 'Giuliano Vassalli' per dottorandi e dottori di ricerca

(AIDP Gruppo Italiano, Siracusa International Institute for Criminal Justice and Human Rights – Siracusa, 29 novembre - 1° dicembre 2018)

ISSN 2240-7618

2/2019

Editore Associazione "Progetto giustizia penale", via Altaguardia 1, Milano - c.f. 97792250157
ANNO 2019 - CODICE ISSN 2240-7618 - Registrazione presso il Tribunale di Milano, al n. 554 del 18 novembre 2011.
Impaginazione a cura di Chiara Pavesi

Diritto penale contemporaneo – Rivista trimestrale è un periodico on line ad accesso libero e non ha fine di profitto. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione. La rivista, registrata presso il Tribunale di Milano, al n. 554 del 18 novembre 2011, è edita attualmente dall'associazione "Progetto giustizia penale", con sede a Milano, ed è pubblicata con la collaborazione scientifica e il supporto dell'Università Commerciale Luigi Bocconi di Milano, dell'Università degli Studi di Milano, dell'Università di Roma Tre, dell'Università LUISS Guido Carli, dell'Universitat de Barcelona e dell'Università Diego Portales di Santiago del Cile.

La rivista pubblica contributi inediti relativi a temi di interesse per le scienze penalistiche a livello internazionale, in lingua italiana, spagnolo, inglese, francese, tedesca e portoghese. Ogni contributo è corredato da un breve abstract in italiano, spagnolo e inglese.

La rivista è classificata dall'ANVUR come rivista scientifica per l'area 12 (scienze giuridiche), di classe A per i settori scientifici G1 (diritto penale) e G2 (diritto processuale penale). È indicizzata in DoGI e DOAJ.

La rivista può essere citata in forma abbreviata con l'acronimo: *DPC-RT*, corredato dall'indicazione dell'anno di edizione e del fascicolo.

La rivista fa proprio il Code of Conduct and Best Practice Guidelines for Journal Editors elaborato dal COPE (Committee on Publication Ethics).

La rivista si conforma alle norme del Regolamento UE 2016/679 in materia di tutela dei dati personali e di uso dei cookies (clicca qui per dettagli).

Ogni contributo proposto per la pubblicazione è preliminarmente esaminato dalla direzione, che verifica l'attinenza con i temi trattati dalla rivista e il rispetto dei requisiti minimi della pubblicazione.

In caso di esito positivo di questa prima valutazione, la direzione invia il contributo in forma anonima a due revisori, individuati secondo criteri di rotazione tra i membri dell'Editorial Advisory Board in relazione alla rispettiva competenza per materia e alle conoscenze linguistiche. I revisori ricevono una scheda di valutazione, da consegnare compilata alla direzione entro il termine da essa indicato. Nel caso di tardiva o mancata consegna della scheda, la direzione si riserva la facoltà di scegliere un nuovo revisore.

La direzione comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se entrambe le valutazioni sono positive, il contributo è pubblicato. Se una o entrambe le valutazioni raccomandano modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se uno o entrambi i revisori esprimono parere negativo alla pubblicazione.

La direzione si riserva la facoltà di pubblicare, in casi eccezionali, contributi non previamente sottoposti alla procedura di peer review. Di ciò è data notizia nella prima pagina del contributo, con indicazione delle ragioni relative.

Se desideri proporre una pubblicazione alla nostra rivista, invia una mail a editor.criminaljusticenetwork@gmail.com. I contributi che saranno ritenuti dalla direzione di potenziale interesse per la rivista saranno sottoposti alla procedura di peer review sopra descritta. I contributi proposti alla rivista per la pubblicazione dovranno rispettare i criteri redazionali scaricabili qui.

Diritto penale contemporaneo – Rivista trimestrale es una publicación periódica *on line*, de libre acceso y sin ánimo de lucro. Todas las colaboraciones de carácter organizativo y editorial se realizan gratuitamente y no se imponen a los autores costes de maquetación y publicación.
La Revista, registrada en el Tribunal de Milan, en el n. 554 del 18 de noviembre de 2011, se edita actualmente por la asociación "Progetto giustizia penale", con sede en Milán, y se publica con la colaboración científica y el soporte de la *Università Commerciale Luigi Bocconi* di Milano, la *Università degli Studi di Milano,* la *Università di Roma Tre*, la *Università LUISS Guido Carli*, la *Universitat de Barcelona* y la *Universidad Diego Portales de Santiago de Chile.*
La Revista publica contribuciones inéditas, sobre temas de interés para la ciencia penal a nivel internacional, escritas en lengua italiana, española, inglesa, francesa, alemana o portuguesa. Todas las contribuciones van acompañadas de un breve abstract en italiano, español e inglés.
El lector puede leer, compartir, reproducir, distribuir, imprimir, comunicar a terceros, exponer en público, buscar y señalar mediante enlaces de hipervínculo todos los trabajos publicados en "Diritto penale contemporaneo – Rivista trimestrale", con cualquier medio y formato, para cualquier fin lícito y no comercial, dentro de los límites que permite la licencia *Creative Commons - Attribuzione - Non commerciale 3.0 Italia* (CC BY-NC 3.0 IT) y, en particular, debiendo mantenerse la indicación de la fuente, el logo, el formato gráfico original, así como el autor de la contribución.
La Revista se puede citar de forma abreviada cn el acrónimo *DPC-RT*, indicando el año de edición y el fascículo.
La Revista asume el Code of Conduct and Best Practice Guidelines for Journal Editors elaborado por el COPE (*Comitte on Publication Ethics*).
La Revista cumple lo dispuesto en el Reglamento UE 2016/679 en materia de protección de datos personales (clica aquí para los detalles sobre protectión de la privacy y uso de cookies).
Todas las contribuciones cuya publicación se propone serán examinadas previamente por la Dirección, que verificará la correspondencia con los temas tratados en la Revista y el respeto de los requisitos mínimos para su publicación.
En el caso de que se supere con éxito aquella primera valoración, la Dirección enviará la contribución de forma anónima a dos evaluadores, escogidos entre los miembros del *Editorial Advisory Board*, siguiendo criterios de rotación, de competencia por razón de la materia y atendiendo también al idioma del texto. Los evaluadores recibirán un formulario, que deberán devolver a la Dirección en el plazo indicado. En el caso de que la devolución del formulario se retrasara o no llegara a producirse, la Dirección se reserva la facultad de escoger un nuevo evaluador.
La Dirección comunicará el resultado de la evaluación al autor, garantizando el anonimato de los evaluadores. Si ambas evaluaciones son positivas, la contribución se publicará. Si alguna de las evaluaciones recomienda modificaciones, la contribución se publicará después de que su autor la haya revisado sobre la base de los comentarios recibidos y de que la Dirección haya verificado que tales comentarios han sido atendidos. La contribución no se publicará cuando uno o ambos evaluadores se pronuncien negativamente sobre su publicación.
La Dirección se reserva la facultad de publicar, en casos excepcionales, contribuciones que no hayan sido previamente sometidas a *peer review*. Se informará de ello en la primera página de la contribución, indicando las razones.

Si deseas proponer una publicación en nuestra revista, envía un mail a la dirección editor.criminaljusticenetwork@gmail.com. Las contribuciones que la Dirección considere de potencial interés para la Revista se someterán al proceso de *peer review* descrito arriba. Las contribuciones que se propongan a la Revista para su publicación deberán respetar los criterios de redacción (se pueden descargar aquí).

Diritto penale contemporaneo – Rivista trimestrale is an on-line, open-access, non-profit legal journal. All of the organisational and publishing partnerships are provided free of charge with no author processing fees. The journal, registered with the Court of Milan (n° 554 - 18/11/2011), is currently produced by the association "Progetto giustizia penale", based in Milan and is published with the support of Bocconi University of Milan, the University of Milan, Roma Tre University, the University LUISS Guido Carli, the University of Barcelona and Diego Portales University of Santiago, Chile.

The journal welcomes unpublished papers on topics of interest to the international community of criminal scholars and practitioners in the following languages; Italian, Spanish, English, French, German and Portuguese. Each paper is accompanied by a short abstract in Italian, Spanish and English.

For citation purposes the journal's abbreviated reference format may be used: *DPC-RT,* indicating year of publication and issue.

The journal strictly adheres to the Code of Conduct and Best Practice Guidelines for Journal Editors drawn up by COPE (Committee on Publication Ethics).

The journal complies with the General Data Protection Regulation (EU) 2016/679 (GDPR) (click here for details on protection of privacy and use of cookies).

All articles submitted for publication are first assessed by the Editorial Board to verify pertinence to topics addressed by the journal and to ensure that the publication's minimum standards and format requirements are met.

Should the paper in question be deemed suitable, the Editorial Board, maintaining the anonymity of the author, will send the submission to two reviewers selected in rotation from the Editorial Advisory Board, based on their areas of expertise and linguistic competence. The reviewers are provided with a feedback form to compile and submit back to the editorial board within an established timeframe. If the timeline is not heeded to or if no feedback is submitted, the editorial board reserves the right to choose a new reviewer.

The Editorial Board, whilst guaranteeing the anonymity of the reviewers, will inform the author of the decision on publication. If both evaluations are positive, the paper is published. If one or both of the evaluations recommends changes the paper will be published subsequent to revision by the author based on the comments received and verification by the editorial board. The paper will not be published should one or both of the reviewers provide negative feedback.

In exceptional cases the Editorial Board reserves the right to publish papers that have not undergone the peer review process. This will be noted on the first page of the paper and an explanation provided.

If you wish to submit a paper to our publication please email us at editor.criminaljusticenetwork@gmail.com. All papers considered of interest by the editorial board will be subject to peer review process detailed above. All papers submitted for publication must abide by the editorial guidelines (download here).

Contents

Contents

Financial cybercrime

Cibercrimen financiero

Financial Cybercrime

Contents

La tutela penale della privacy nel cyberspazio

La tutela penal de la privacidad en el ciberespacio

Criminal Law and the Protection of Privacy in Cyberspace

Contents

Contents

Contents

La tutela penale della privacy nel cyberspazio

La tutela penal de la privacidad en el ciberespacio

Criminal Law and the Protection of Privacy in Cyberspace

I limiti della tutela penale del trattamento illecito dei dati personali nel mondo digitale

Los límites de la tutela penal del tratamiento ilícito de datos personales en el mundo digital

Limits to Criminalization of Unlawful Data Processing in the Digital World

Salvatore Orlando
Dottore di ricerca in Diritto penale presso l'Università di Palermo
salvatore.orlando@unipa.it

Privacy, Dolo Privacy, Dolo Privacy, Intention

Abstracts

L'incessante scambio di dati ed informazioni nel mondo del web ha imposto una rivisitazione dei paradigmi classici del bene giuridico della *privacy*. Emblematico è, in tal senso, il reato di *trattamento illecito dei dati personali*, di cui all'art. 167 Codice *privacy* (D. Lgs. 196/2003), oggetto di numerosi interventi correttivi per adeguarlo alle moderne e mutevoli esigenze di tutela. L'indagine riflette dunque sulla recente riforma (D. Lgs. 101/2018) che sembra voler recuperare l'offensività del tipo delittuoso attraverso la formulazione di un reato di evento il cui disvalore è incentrato sul *nocumento all'interessato:* tuttavia, in modo apparentemente inconciliabile, viene mantenuto un *dolo specifico di danno*, che si sovrappone al risultato materiale conseguito dall'agente. Infine, si cerca di dimostrare come stia emergendo una nuova oggettività giuridica di carattere pubblicistico, ossia il *sistema di protezione dei dati personali*, la cui tutela è demandata agli artt. 167-*bis* e 167-*ter*.

El permanente intercambio de datos e informaciones en el mundo de la web ha impuesto una revisión de los paradigmas clásicos de la privacidad como bien jurídico. El delito de tratamiento ilícito de datos personales, establecido en el art. 167 del Código de la Privacidad (Decreto Legislativo 196/2003), es emblemático en este sentido, habiendo sido objeto de numerosas modificaciones para adaptarlo a las necesidades modernas y cambiantes de protección. El presente trabajo reflexiona sobre la reciente reforma legislativa (Decreto Legislativo 101/2018), la cual pareciera intentar recuperar la lesividad del tipo penal a través de la formulación de un delito de resultado cuya lesión se centra en el daño a la persona afectada. Sin embargo, de forma aparentemente irreconciliable, se mantiene un animo específico de daño, que se solapa con el resultado material conseguido por el agente. Por último, se intenta demostrar cómo está surgiendo una nueva objetividad jurídica de carácter publico, es decir, el sistema de protección de datos personales, cuya protección se reserva a los artículos 167-bis y 167-ter.

The constant exchange of data and information in the world of the web has imposed a reinterpretation of the classic paradigms related to the so-called *privacy* as a legal interest. The crime of unlawful processing of personal data, as per art. 167 of the Italian Privacy Code (Legislative Decree 196/2003), is emblematic in this sense, and has been emended by numerous corrective measures in order to adapt it to the modern and changing needs of legal protection. The analysis carried out here therefore reflects on the recent reform (Legislative Decree 101/2018) which tries to recover the offensiveness of the criminal type through the formulation of a result crime whose offence is focused on the *harm* to the person concerned: however, in an apparently irreconcilable way, *a*

specific intent of damage is maintained, which overlaps with the material result achieved by the agent. Finally, the paper tries to demonstrate how a new legal interest with a public nature is emerging, that is, the *system of protection of personal data*, the protection of which is entrusted to Articles 167-bis and 167-ter.

Sommario

1. Profili introduttivi.

Il mondo delle connessioni digitali è pervaso da un *fil rouge* che virtualmente unisce gli utenti del *web* in un incessante scambio di informazioni, veicolate attraverso piattaforme immateriali. È noto come, al fine di essere parte di una comunità digitale, sia necessario comunicare i *propri dati personali* i quali, secondo dinamiche che rispondono ad algoritmi non intelligibili ai più, creano il nostro profilo identificativo nel *web*: in questo momento, abbiamo rinunciato *consensualmente* alla nostra assoluta signoria ed al controllo sui nostri dati personali[1].

Infatti, in una società ad altissima – e ancora crescente – informatizzazione delle attività e dei servizi, è inevitabile per ciascuno di noi la necessità di lasciare una traccia della propria attività, delle abitudini, delle caratteristiche e delle preferenze personali. Chi raccoglie i dati ricevuti procede poi al loro trattamento con finalità, tra le altre, di c.d. *profilazione* nell'ambito di attività di *marketing* o di classificazione dei cittadini che, in ultima istanza, possono prestarsi ad usi discriminatori o per scopi elettorali.

Ed in questo senso, sorgono evidenti questioni di tutela della c.d. *privacy* o più propriamente riservatezza. Sul tema la letteratura è sterminata: si parla talora di *privacy*, talaltra di *privatezza*, ovvero di *vita privata*, o ancora di *riservatezza*, alludendo a concetti non sempre coincidenti[2]. In particolare, la nozione di *privacy* – come "*diritto dell'età d'oro della borghesia*"[3] – fa il primo ingresso in Italia soltanto nel 1970 attraverso l'art. 8 dello Statuto dei lavoratori[4] che vieta la raccolta delle opinioni politiche, sindacali, religiose dei dipendenti.

Tuttavia, nel corso degli ultimi decenni il bene oggetto di tutela penale, dapprima dotato di una forte connotazione individualistica, è andato assumendo via via una natura pubblicistica, appuntandosi ormai, come meglio si vedrà, sul piano della *protezione dei dati personali*[5].

In questo breve contributo si intende, da un lato, illustrare criticamente i profili giuridici più significativi e i limiti della tutela penale che il legislatore ha dovuto affrontare – con risultati certo altalenanti – nella formulazione di tipi delittuosi diretti alla tutela del bene della *privacy;* dall'altro lato, segnalare le aporie del sistema di tutela apprestato e, dunque, vagliare attentamente le soluzioni ermeneutiche offerte dalle Corti, che – seppur in sporadiche decisioni – hanno ricostruito la *ratio legis* di protezione di un bene giuridico tanto di recente emersione, quanto di notevole rilevanza nel contesto contemporaneo e prevedibilmente ancora crescente in futuro.

In questo senso, constatata dapprima l'evoluzione concettuale della *privacy* ed evidenziati i possibili profili di interesse penalistico – seppur, si avverte, soltanto marginali all'interno del *mare magnum* degli aspetti riconducibili al tema – ci si concentra sui problemi di tecnica legislativa. In relazione infatti ad una tutela che trova incontestabile legittimità sul versante costituzionale, numerose questioni sorgono al momento di individuarne tanto i limiti quanto gli strumenti di attuazione, nella correlata prospettiva del rispetto dei principi di materialità, determinatezza ed offensività, nonché della effettività della risposta giuridica. La complessità della materia è testimoniata dal '*travaglio legislativo*' che ha segnato il nostro ordinamento in tema di tutela della *privacy,* il quale trova esemplificazione nelle notevoli modifiche appor-

[1] In relazione ai notevoli rischi (non solo incidenti sull'interesse penalmente rilevante della *privacy*) dei c.d. *Social Network*, ossia delle piattaforme web di condivisione di dati, informazioni e notizie personali, si veda, Picotti (2012), p. 2522; altresì, Galdieri (2012), p. 2697.
[2] Bricola (1967), 1114.
[3] Così, Rodotà (2005), 12.
[4] L. 20 maggio 1970, n. 300 "*Norme sulla tutela e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento*".
[5] In ambito penalistico, il riferimento alla riservatezza come bene degno di tutela viene introdotto con la Legge 8 aprile 1974, n. 98 "*Tutela della riservatezza e della libertà e segretezza delle comunicazioni*", che introduce alcune fattispecie delittuose tra le quali, l'art. 615-bis *Interferenze illecite nella vita privata,* inserito nel capo III, sez. IV (Delitti contro la inviolabilità del domicilio) titolo XII (Delitti contro la persona), l'art. 617-bis *Installazione di apparecchiature atte a intercettare o impedire comunicazioni telegrafiche o* telefoniche, e l'art. 617-ter *Falsificazione, alterazione o soppressione di contenuto di comunicazioni o conversazioni telegrafiche o telefoniche.*

tate alla fattispecie di *trattamento illecito dei dati personali*, di cui all'art. 167 del Codice della *privacy*[6]. Come meglio si cercherà di dimostrare nel corso dell'indagine, la norma è costruita secondo una progressione criminosa attenta a selezionare le condotte meritevoli di punizione attraverso il dolo specifico e, con l'ultima modifica intervenuta con il D. Lgs. 101/2018, configura un reato di evento il cui disvalore appare incentrato sulla lesione ad un bene individuale, mediante il ricorso all'espressione del "*nocumento all'interessato*". Pur tuttavia, a seguito della riforma, il fuoco dell'incriminazione si sposta verso una nuova oggettività giuridica (meglio, un bene-categoria) di carattere pubblicistico, ossia il *sistema di protezione dei dati personali*, la cui tutela è demandata ora agli articoli 167-*bis* e 167-*ter*.

2. La *Privacy*: possibili profili penalistici in un mondo digitale.

Orbene, in primo luogo, appare possibile – nonché opportuno – distinguere i concetti di *privacy* o riservatezza[7] e quello di diritto alla protezione dei dati personali, i quali indicherebbero oggettività giuridiche tra loro in parte differenti: è, infatti, preliminare vagliare il significato dell'interesse che si intende salvaguardare nonché gli scopi di tutela perseguiti attraverso lo strumento penale[8].

Il concetto di *privacy* viene elaborato per la prima volta nell'Ottocento nel mondo anglosassone – in cui storicamente più alto è stato il "*grado di sensibilizzazione*" in materia[9] – da parte di due giuristi, Warren e Brandeis[10], che ne hanno individuato il nucleo costitutivo nel celeberrimo *right to be let alone*, il diritto di essere lasciato da solo. In questo senso, in una accezione ancora primordiale ma mai veramente superata, si tentava di porre l'accento su quell'innata esigenza dell'uomo di escludere gli altri dalla conoscenza di sé stessi e della propria sfera personale. È alquanto curioso come – seppur in un contesto non ancora globalizzato e affatto digitalizzato – questa esigenza si manifestasse in aspetti solo in parte differenti da quelli che oggi rilevano, come ad esempio, nella segretezza della corrispondenza o nella non diffusione di fotografie a mezzo stampa. Questa esigenza dunque – che potenzialmente può rivolgersi tanto ai poteri pubblici quanto alle interferenze private – si è andata evolvendo, lasciando tuttavia in eredità problemi definitori in ordine alla individuazione di una nozione univoca di *privacy*. Così, si è andato delineando un '*catalogo aperto*' che riguardasse, in generale, la tutela della sfera privata dell'individuo: la necessità di limitare l'accesso di altri alla propria sfera personale; il diritto di tenere determinate questioni segrete agli altri; la tutela della propria personalità, identità e dignità; il diritto all'intimità, ossia al riserbo circa le proprie relazioni personali o determinati aspetti della propria vita[11].

Della *privacy* quale oggetto di tutela si è soliti individuare un duplice contenuto[12]: un nucleo originario e tradizionale, afferente per l'appunto al c.d. *right to be let alone*, dal quale discende il diritto alla conoscenza esclusiva delle vicende relative alla propria vita privata (ovvero, da altra prospettiva, all'assenza di informazioni su noi stessi da parte degli altri); e un interesse al controllo esterno dei propri dati personali, in funzione di una corretta utilizzazione degli stessi[13].

In quest'ultimo senso, dunque è possibile già scorgere una *dimensione sociale della privacy* che si aggiunge al tradizionale aspetto individualistico della medesima e che riguarderebbe il problema del corretto e trasparente trattamento dei dati personali, che può manifestarsi in una duplice direzione: da un lato, si profilerebbe con un contenuto c.d. negativo (si suole dire,

[6] Ossia, il D. Lgs. 30 giugno 2003, n. 196, il quale, a seguito dell'ultima riforma intervenuta con il D. Lgs. 101/2018 (cfr. *infra* par. 4), è intitolato "*Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*".

[7] Nel senso di una totale coincidenza dei due concetti, Pizzetti (2016), p. 45. Sul rapporto tra *privacy* e diritto alla riservatezza, da ultimo si v. Manna, Di Florio (2019), p. 892.

[8] Sul punto, il quesito era stato posto, già a seguito della prima riforma in materia, su cui *infra* par. 3., da Sgubbi, (1998), p. 75.

[9] Cosi, Bricola (1967), p. 1081.

[10] Warren e Brandeis (1890), p. 193.

[11] In questi termini, si veda, Lamanuzzi (2017), p. 221.

[12] Patrono (1986), p. 557 s.

[13] Sui profili problematici tra diritto alla riservatezza e libertà di informazione, e dunque di divulgazione di notizie afferenti alla vita privata, si veda, tra gli altri, Vigevani (2016), p. 473. Non v'è dubbio, peraltro, che nel mondo digitale la dualità si pone in termini differenti, in quanto il *web* si configura come uno spazio di deresponsabilizzazione e, per certi versi, come un *freies Raumrecht*.

libertà da), che ricomprenderebbe il diritto a mantenere il riserbo su certi dati, o comunque a limitarne la circolazione latamente intesa (il che atterrebbe ancora alla riservatezza *strictu sensu*); dall'altro lato, avrebbe, invece, un contenuto positivo (si suole dire, *libertà di*), che assumerebbe una valenza poliedrica, dovendo essere garantiti alla *platea di interessati* (si noti, fin d'ora, l'ampiezza dei titolari) i mezzi (ad es., l'accesso e la cancellazione) necessari alla correttezza del trattamento degli stessi, al fine di salvaguardare, in primo luogo, l'identità personale di coloro ai quali i dati si riferiscono[14].

In questo variegato contesto, si staglia nella *materia penalistica* il lavoro di Franco Bricola[15], il quale oltre mezzo secolo fa parlava della riservatezza e della sua rilevanza sociale già in termini preoccupati, riservando la sua trattazione alle possibili interferenze nella vita privata, con specifico riguardo ai profili di interesse pubblico alla non diffusione delle informazioni personali.

In questo senso – avendo definito la stampa e la televisione mezzi idonei all'espropriazione *per pubblica curiosità* – distingueva tre sfere più particolari della vita privata, in contrapposizione all'interesse alla *vita di relazione*, in cui rientrerebbe la tutela della reputazione[16]: la sfera privata *strictu sensu* (*Privatsphäre*) che ricomprende tutti quei comportamenti, notizie o informazioni che il soggetto *desidera* non divengano di pubblico dominio; la sfera confidenziale (*Vertrauensphäre*) che ricomprende quegli avvenimenti, discorsi o notizie di cui il soggetto rende partecipi persone di particolare fiducia; e infine, la sfera del segreto (*Geheimsphäre*) che ricomprende tutte quelle notizie e fatti che per interessi o ragioni particolari sono inaccessibili a chiunque non sia titolare del segreto (e ne abbiano dunque ricevuto il consenso). Le tre sfere possono immaginarsi come tre cerchi concentrici di raggio progressivamente minore e ad esse la dottrina ha fatto riferimento, quando ha affrontato il tema del diritto alla riservatezza.

In questo contesto, merito del lavoro di Bricola è quello di iniziare a distinguere due momenti in cui sussisterebbe un bisogno di tutela penale: il momento delle *interferenze esterne* nella sfera privata che è presidiato dal diritto al rispetto alla vita privata, nel senso dunque più pregnante; ed il momento della *diffusione* e *divulgazione* di notizie e informazioni, ancorché legittimamente acquisite, la cui difesa spetterebbe, invece, al diritto alla riservatezza. E, con riferimento a quest'ultimo, si spinge ad un ulteriore *discrimen*, che sembra anticipare ed ispirare le scelte incriminatrici più recenti: egli distingue, da un lato, tra la violazione del segreto che sussisterebbe nel caso di conoscenza illegittima (dunque, senza consenso) di dati confidenziali racchiusi, ad esempio, nella corrispondenza e, dall'altro, la violazione del diritto alla riservatezza che si ha nel caso di rivelazione a terzi della notizia da parte del soggetto destinatario della fiducia.

La demarcazione è sottile, ma estremamente utile ai fini del corretto inquadramento dell'attuale sistema di tutela della *privacy*, nella sua declinazione di *protezione dei dati personali*, che si insinuerebbe in questo reticolo concettuale, per l'appunto, tra la tutela del segreto della vita privata[17], quest'ultimo inteso nel senso più ampio, e la tutela della riservatezza, ossia nell'interesse alla *non diffusione* di informazioni relative alla propria sfera privata[18]. Ed è dunque tenendo conto di questa ambivalenza che deve essere intesa l'evoluzione recente della legislazione in materia di *privacy*[19].

In questo senso, si è mossa anche la costruzione di una tutela penale che – in una prospettiva sostanzialistica – ha tentato di dare rilievo ad un valore – quello della riservatezza – avente originariamente un forte *margine di relatività*, in relazione alla diversa sensibilità ed esigenze che può legittimamente avere il titolare, ma che, a ben vedere, atteso un nucleo essenziale "*costante per la media dei cittadini*", si pone tra la rilevanza scriminante del consenso e l'interesse

[14] Si veda, Veneziani (2001), p. 369.
[15] Bricola (1967), p. 1114 ss.; illuminanti altresì i contributi di Mantovani (1968), p. 61 ss.; Palazzo (1975), p. 126 ss.
[16] L'interesse alla reputazione è tutelato dall'art. 594 c.p. che punisce il reato diffamazione. A ben vedere, l'interesse alla vita di relazione e l'interesse alla vita privata possono sussistere nello stesso caso concreto ed in tal senso possono sorgere problemi di concorso di reati, sul punto cfr. Carnelutti (1955), p. 5 s.
[17] A tal proposito, ma si tornerà anche in seguito, cfr. Cass. Pen., Sez. VI, 21.02.2013, n. 9726, in relazione alla rivelazione ed utilizzazione di segreti di ufficio.
[18] Sul punto, si può vedere altresì il recente lavoro di D'Agostino (2019), in part. 5 ss.
[19] Negli ultimi anni la nozione di *privacy* è stata invocata in una accezione funzionale che tende a distanziarla da quella di riservatezza e ad identificarla con il diritto protezione dei dati personali. La sovrapposizione che si registra – tra *privacy* e protezione dei dati personali – è dovuta principalmente al fatto che la legge organica che contiene la sua disciplina va sotto il nome di codice della privacy e l'autorità preposta alla sua corretta implementazione Garante della *privacy*. Quindi, convenzionalmente, viene il termine privacy nel senso di protezione dei dati personali, il quale sottende ovviamente anche un interesse generale a che la circolazione dei dati avvenga in modo lecito e trasparente senza finalità ulteriori di propaganda politica o di marketing, cfr. Pizzetti (2016), 45.

pubblico alla divulgazione delle notizie.

Così, in un percorso storico-penalistico, in cui i concetti di valore come la reputazione ed il decoro[20] hanno cominciato a segnare una rinuncia allo strumento penale[21], la tutela della *privacy* – seppur strettamente legata a questi ultimi[22] – ha, invece, mutato i propri fini e le tecniche di incriminazione[23].

3. La tutela della *privacy* all'insegna di un diritto penale emergenziale

Ad una valutazione d'insieme, l'osservatore della materia non può non accorgersi che il sistema penale di tutela della *privacy* appare caratterizzato, fin dalle sue embrionali formulazioni, dal ricorso, in via emergenziale e rapsodica, a strumenti sanzionatori nuovi e a costruzioni di tipi delittuosi censurabili di incostituzionalità.

In un panorama in cui si stagliano sullo sfondo le sfide delle nuove e problematiche frontiere tecnologiche[24], il diritto penale ha reagito per lo più in modo disarmonico e disorganico fino ad assumere il volto di una *legislazione emergenziale*. Ciò si evince dal tentativo del legislatore di reprimere *tout court* le condotte indesiderabili, anticipando le soglie di punibilità o formulando fattispecie di pericolo[25].

Come noto, la natura frammentaria del diritto penale è frutto di una società tradizionale e di schemi di comportamento familiari alla coscienza sociale. Il legislatore, invero, tanto nell'ottica dell'armonizzazione comunitaria imposta dalla Direttiva 95/46/CE[26], quanto nella prospettiva di massima repressione dei nuovi fenomeni emersi nel mondo del digitale che avevano suscitato grande allarme sociale, ha, invece, tentato di abbracciare tutte le ipotesi possibili, formulando tipi delittuosi connotati da indeterminatezza e genericità, anticipando la punibilità a ipotesi di mera messa in pericolo del bene tutelato.

Un fenomeno collegato a tale constatazione è quello dell'emersione di una *nuova funzione al giudice penale*, il quale – si può dire, *obtorto collo* – crea diritto: nel caso della tutela della *privacy*, lo si vedrà meglio con riguardo al trattamento illecito dei dati personali, il legislatore affida al giudice l'individuazione dell'ambito realmente appropriato di applicazione della legge. In questo senso, il diritto penale, facendo ricorso ad una legislazione simbolica, demanda alla prassi giudiziaria – ossia al "diritto vivente" – l'onere di provvedere alla sua efficienza[27].

Ciò premesso, al fine porre rimedio a costruzioni legislative esposte a rischi tanto di inefficacia quanto di incostituzionalità, è preliminare affrontare la questione circa la possibile individuazione di un bene-categoria[28], al quale riferire l'offesa in maniera sostanzialmente uniforme dal punto di vista del tipo di interesse tutelato: nella materia *de qua* appare oggi pacifico che la rilevanza costituzionale dell'interesse della riservatezza sembra essere ancorato all'art.

[20] Sui possibili collegamenti tra disciplina della *privacy* e reputazione, si veda, Seminara (1998), p. 911. Inoltre, mai superate le riflessioni di Musco (1974), in part. p. 133 s.

[21] Si pensi, a titolo esemplificativo, alla parziale depenalizzazione in materia di atti osceni, di cui all'art. 527 c.p. che oggi prevede una sola sanzione pecuniaria amministrativa, a seguito dell'introduzione del D. Lgs. 8/2016; si pensi, altresì, al reato di ingiuria che è stato depenalizzato con il D. Lgs. 7/2016.

[22] Sul punto, si veda Manna (1998), p. 260.

[23] Scrive Fiore (1999), p. 1 che "[…] *nel mondo contemporaneo, la riservatezza, quale espressione tanto del diritto della personalità quanto del bene dell'onore, ha svolto il ruolo di una sorta di estremo baluardo eretto per l'appunto contro l'erosione del valore dell'individualità in una società fortemente orientata all'omologazione dei comportamenti sociali e degli atteggiamenti culturali e quindi ad alto rischio di discriminazione*".

[24] Cfr. per una panoramica generale sui nuovi "rischi" della tecnologia e dell'informatica, si v., per tutti, Militello e Spena (2018).

[25] Cfr. Grasso (1986), p. 689 ss.; Marinucci (1987), p. 19 s.; Pulitanò (1987), p. 33 s.; Canestrari (1991), p. 7 ss.; Angioni (1994); M. Romano (1995), p. 319 s.; Parodi Giusino (1999), p. 687 ss. Altresì sul punto, sono interessanti le riflessioni in materia ambientale, che, per quanto concerne la tutela penale apprestata, appare per certi versi affine alla materia che è oggetto della presente indagine, cfr. Giunta (1997), p. 1102.

[26] Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 "*relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati*".

[27] Ad esempio, Troncone (2014), p. 2066, secondo cui il reato sul trattamento illecito dei dati personali sarebbe "*una norma laboratorio*", da cui discendono "*le problematiche dei più significativi nodi teorici del diritto penale ma anche il legislatore non ha munito di quei dispositivi per risolvere le ipotesi applicative controverse*".

[28] Nonostante – fuori da una legislazione penale organica non dotata di funzioni sistematiche – sia difficile che la *ratio legis* di ogni singola norma possa contribuire a comporre uno scopo di tutela unitario: in questo senso, si vedano le osservazioni di Pagliaro (1965), p. 389 s., che propende per una "nozione metodologica del bene tutelato" che, valorizzando la *ratio* di ogni singola norma incriminatrice, si discosta dalla della possibilità di individuazione di un oggetto giuridico di categoria.

2 della Costituzione, la cui natura di 'clausola aperta' ne consente il pieno riconoscimento[29], ed altresì all'art. 7 della Carta di Nizza[30] ed all'art. 8 della Convenzione Europea dei diritti dell'uomo[31], norme che come è noto trovano ingresso nel nostro ordinamento rispettivamente attraverso gli artt. 11 e 117 Cost.

Orbene, acquisito questo dato – certamente necessario, ma non ancora sufficiente per ancorare una protezione penalistica – si pone il quesito principale sui limiti della tutela da apprestare al bene giuridico della *privacy*, nella sua declinazione, come visto, della *protezione dei dati personali*. In altri termini, assodata la legittimità sul versante costituzionale della tutela penale della riservatezza, il problema si sposta – e per vero, come sempre, diviene delicato – nel momento nel quale da quest'assunzione di carattere generale e generico si deve passare alla concreta definizione degli strumenti di tutela, che possono legittimare l'intervento repressivo nell'ottica del rispetto dei principi di sussidiarietà, determinatezza e offensività[32].

In un contesto in cui si è passati da una tendenza all'espansione dell'intervento penale[33], soprattutto in campi emergenti come quelli dell'economia e del mondo digitale, si è da ultimo giunti ad una prospettiva legislativa di depenalizzazione e dunque di arretramento dell'area del penalmente rilevante.

Ed in questo senso, soprattutto in epoche di grandi tensioni sociali o di emergenze repressive, l'obiettiva difficoltà di determinare i caratteri essenziali degli oggetti di tutela e dunque individuare le condotte idonee ad offenderli ha indotto il legislatore – con la prima forma di incriminazione del trattamento illecito dei dati personali di cui alla L. 675/1996[34] – a percorrere la strada di una forte anticipazione della soglia di punibilità a momenti di *pericolo astratto* o *presunto*, in cui il verificarsi di un danno effettivo – e dunque di un'offesa ad un bene individuale – non era elemento essenziale per l'integrazione della fattispecie e dunque presupposto per la punibilità, ma era tipizzato quale circostanza aggravante, secondo la costruzione di un reato aggravato dall'evento[35].

Con la novella del 1996 – che avrebbe poi rappresentato il modello base su cui il legislatore è intervenuto a più riprese – si puniva "*chiunque, al fine di trarre per sé o per altri profitto o di arrecare ad altri un danno, procede al trattamento di dati personali in violazione degli artt. 11, 20 e 27, è punito con la reclusione sino a 2 anni o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da tre mesi a due anni*" (art. 35).

Con una infelice formulazione legislativa, dunque veniva introdotto un mero delitto di infedeltà o di inottemperanza[36] il cui disvalore era tutto incentrato sulla violazione degli artt. 11, 20 e 27 della stessa legge[37]: in questo senso non veniva costruita una fattispecie incriminatrice dotata di un contenuto materiale afferrabile e la cui modalità di aggressione al bene-categoria individuato non sembrava poggiare su solide basi, in quanto la fattispecie – si lamentava – era strutturata come *clausola sanzionatoria dei precetti extrapenali*[38].

[29] Per tutti, Bricola (1967), p. 1114; più di recente altresì Troncone (2011), p. 23 s. In giurisprudenza, cfr. Cass. sez. III, 9 giugno 1998, n. 5658, che definisce la riservatezza un «*diritto soggettivo perfetto*», che protegge «*situazioni e vicende strettamente personali, ancorché verificatesi fuori dal domicilio domestico, da ingerenze che, sia pure compiute con mezzi leciti e senza arrecare danno all'onore, al decoro o alla reputazione, non siano tuttavia giustificate da un interesse pubblico preminente*» e ricava la tutela costituzionale della vita privata di un soggetto dal complesso dei principi della Carta e dunque, oltre che dall'art. 2, anche dall'art. 3 e dagli artt. 14, 15, 27, 29 e 41 Cost.

[30] Art. 7 Rispetto della vita privata e della vita familiare: "*Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni*".

[31] Art. 8 *"1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui*

[32] Così, altresì Mucciarelli (2004), p. 173; cfr. Fiore (1999).

[33] Parla di "panpenalismo", invece, Manna (1993), p. 179 s.

[34] La legge n. 675 del 1996 ha rappresentato il primo sostanziale intervento direttamente finalizzato a regolamentare in maniera organica il diritto alla riservatezza e le modalità della sua tutela. La legge, anche per dare attuazione a sollecitazioni provenienti da fonti europee (in particolare la direttiva 95/46/CE *Tutela delle persone fisiche con riferimento al trattamento dei dati personali e alla loro libertà di circolazione*) esordiva con la solenne affermazione secondo cui il trattamento dei dati personali si svolge "*nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale* " (art. 1) ponendo un decisivo punto fermo nella lunga diatriba in ordine alla dimensione costituzionale della riservatezza, in quanto diritto assoluto e fondamentale dell'individuo.

[35] Sulla rilevanza del *nocumento* quale circostanza aggravante del reato, si veda Corrias Lucente (1997), p. 82.

[36] Manna (2001), p. 346.

[37] Ai sensi della L. 675/1996, prima della riforma intervenuta nel 2003, l'art. 11 riguarda il problema del consenso al trattamento. L'art. 12 pone però subito alcune eccezioni alla necessità del consenso e ciò significa come il consenso stesso non sia, in realtà, requisito indefettibile della fattispecie. L'art. 20 concerne i requisiti per la comunicazione e diffusione dei dati, mentre l'art. 27 ha per oggetto il trattamento da parte dei soggetti pubblici.

[38] Veneziani (2001), p. 376.

Peraltro, la disposizione incriminatrice citata si inseriva in un contesto normativo connotato da "*grande oscurità*"[39], in cui era massiccio il ricorso al modello delittuoso a discapito di quello contravvenzionale[40]. Da qui, sono affiorate in dottrina molte perplessità circa l'ancoraggio della fattispecie incriminatrice del trattamento illecito – unitamente alle altre figure di reato introdotte dalla L. 675/1996[41] – alla tutela della *riservatezza*, la cui effettiva lesione non rilevava ai fini della punibilità, ma residuava solo nell'espressione dell'eventuale nocumento, ma ai soli fini dell'aggravamento della pena. D'altronde, la legge citata ha rappresentato uno spartiacque nell'evoluzione concettuale della riservatezza, che – affrancandosi dalla concezione tradizionale risalente agli studi di Bricola – si affacciava al mondo del digitale, assumendo una terminologia differente, per l'appunto *privacy*, con un'accezione funzionale[42] nel senso della protezione dei dati personali, onde specificarne la natura di tutela di *interessi generali* alla non diffusione di informazioni personali ed alla *salvaguardia di mere funzioni*, e segnatamente delle funzioni di controllo e di intervento del Garante per la protezione dei dati[43].

Dunque, le scelte legislative *generaliste* e *panpenalizzanti*[44] in materia venivano state in parte ridimensionate con l'introduzione nel 2003 del c.d. *Codice della Privacy* (ma, in realtà, intitolato "*Codice in materia di protezione dei dati personali*"[45]), che cristallizzava definitivamente il superamento del bene-categoria individuale della riservatezza a favore di una nuova oggettività giuridica, e che fu "*ispirato all'introduzione di nuove garanzie per i cittadini, alla razionalizzazione delle norme esistenti e alla semplificazione*"[46].

Con riferimento alla fattispecie di trattamento illecito dei dati personali, il legislatore del 2003 segnava il passaggio ad un delitto caratterizzato dalla condizione obiettiva di punibilità[47], in cui la punibilità era subordinata alla derivazione dal fatto di un *nocumento*[48]. In questo modo, pur mantenendo il precetto penale del tutto incentrato sulla violazione delle disposizioni di natura extrapenale previste all'interno del nuovo Codice della *Privacy*, la loro mera *disobbedienza* non determinava *per se* l'integrazione del reato, se non fosse stata accompagnata dalla derivazione di un nocumento, considerato in senso lato[49].

Il requisito del *nocumento* assumeva dunque i requisiti di elemento del fatto di reato (e non più mera circostanza aggravante), entrando nella fattispecie tipica[50] quale condizione obiettiva di punibilità c.d. intrinseca[51]. Secondo tale impostazione, l'elemento del nocumento non

[39] Manna (2001), p. 344.
[40] Cfr. sul ruolo degli interessi tutelati per la scelta della natura delle sanzioni, cfr. Padovani (1984), p. 465; Id. (1987), p. 670.
[41] Si fa riferimento all'art. 34 "*omessa o infedele notificazione*", l'art. 36 "*omessa adozione di misure necessarie alla sicurezza dei dati*", in cui si rinviava ad una fonte extrapenale, che sollevava censure per violazione del principio di riserva di legge; e, infine, l'art. 37 "*inosservanza dei provvedimenti del Garante*".
[42] Pizzetti (2016), p. 45.
[43] Veneziani (2001), p. 377, il quale si chiedeva dell'opportunità del ricorso all'illecito penale piuttosto che a quello amministrativo, che appariva più adeguato.
[44] Altresì, Veneziani (2001), p. 372.
[45] D. Lgs. 30 giugno 2003, n. 196.
[46] Il codice mantiene pesanti sanzioni pecuniarie aventi natura amministrativa nelle ipotesi di omessa o inidonea informativa all'interessato (art. 161), omessa o incompleta notificazione (art. 163) e di omessa informazione o esibizione al Garante (art. 164), devolvendo l'applicazione delle stesse sanzioni al Garante, quale organo principe del sistema posto a presidio della riservatezza.
[47] Cfr. *infra*. In dottrina, si veda, tra gli altri Musotto (1936); Pagliaro (1960); Giuliani (1966); Angioni (1989), p. 1140 s.; M. Romano (1992), p. 39 s.; D'Ascola (1993), p. 652 s.; Insolera e Stortoni (2001), p. 413 s.; Bricola (2007), pp. 588 s.; nella manualistica, Pagliaro (2003), p. 393; Antolisei (2003), p. 697; Fiandaca e Musco (2012), p. 813; Mantovani (2017), p. 782.
[48] Cfr. Cass. Pen., Sez. V, 28.09.2011, n. 44940 secondo cui "*Sussiste continuità normativa tra il previgente reato di cui all'art. 35 della L. 675/1996 e la nuova fattispecie incriminatrice introdotta dall'art. 167 D. Lgs. 196 del 2003; né rileva in senso contrario che il nocumento alla persona offesa – previsto da entrambe le fattispecie di reato – costituisca nel reato previgente di pericolo presunto una circostanza aggravante, e condizione obiettiva di punibilità in quello vigente, in quanto quel che rileva è che il fatto (condotta ed elemento psicologico) costituente reato nella normativa previgente lo sia anche in quella vigente*", ed ha precisato che la legge previgente deve ritenersi più favorevole all'imputato, potendo la circostanza aggravante – a differenza della condizione obiettiva di punibilità – costituire oggetto del giudizio di bilanciamento, ex art. 69 c.p. *Conf.* Cass. Pen., Sez. III, 26 marzo 2004, n. 28680.
[49] Non vi era un esplicito ancoraggio del nocumento agli interessi o diritti di un soggetto persona fisica (ossia, ad es., *nocumento all'interessato* ovvero *nocumento agli interessi dell'interessato*), tanto che sarebbe stato plausibile ritenere il concetto di nocumento potenzialmente di portata più ampia rispetto ad una offesa individuale, cfr. Art. 167 Codice della Privacy: "*[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 he 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*".
[50] In questo senso, Pagliaro (1960); Id. (2003), p. 394. *Contra* Antolisei (2003), p. 697; altresì Mantovani (2017), p. 782, secondo i quali le condizioni obiettive di punibilità non entrerebbero a far parte della tipicità della fattispecie.
[51] Esempi di condizione obiettiva di punibilità si rinvengono nell'Art. 423 cpv., Art. 580 c.p., Art. 640 c.p.; in dottrina, con riguardo al piano degli interessi tutelati, si è distinta una condizione obiettiva di punibilità c.d. intrinseca (accadimento lesivo del bene protetto) da

avrebbe dovuto rappresentare oggetto del dolo, così da non restringere oltremodo l'area del penalmente rilevante, seppur fosse necessario, non essendo elemento estraneo (ma, appunto, intrinseco) al piano dell'offesa – nel rispetto del principio di colpevolezza come scolpito dagli insegnamenti della Corte Costituzionale[52] – quel *minimum* psicologico ravvisabile nella prevedibilità del fatto offensivo per l'imputabilità del reato a titolo di colpa[53].

In effetti, sarebbe stato *incongruo* prevedere quale evento del reato – e dunque oggetto del dolo – proprio la concretizzazione del fine di danno perseguito dal soggetto, che, in quanto riconducibile ai caratteri del dolo specifico, non è necessario che si realizzi ai fini della consumazione del reato[54].

Nel senso di una condizione obiettiva di punibilità intrinseca deponeva poi la stessa *ratio* della fattispecie che, onde prevenire la punizione di fatti non concretamente lesivi del bene individuale della *privacy*, richiederebbe che dalla condotta – già di per sé illecita perché in violazione del precetto extrapenale richiamato *per relationem* – sia derivata un'offesa dell'interesse protetto "*che è già potenzialmente realizzata dal fatto in senso stretto*"[55].

Orbene, come ha riconosciuto la stessa Corte di Cassazione[56] "*la modifica più evidente apportata dal d.lgs. n. 196/2003 all'art. 35 l. n. 675/96 (ora art. 167) consiste sul piano strutturale nella previsione nella fattispecie-base dell'elemento del "nocumento", attraverso la locuzione "se dal fatto deriva nocumento", precedentemente costituente soltanto una circostanza aggravante*», con la conseguenza che il delitto di illecito trattamento di dati veniva trasformato da reato di pericolo astratto o presunto a quello di pericolo concreto o 'effettivo', per il necessario accertamento della lesione al bene tutelato[57].

La riforma legislativa è sintomatica del cambio di prospettiva del legislatore delegato che ha tentato di riaffermare l'offensività del tipo delittuoso e di agganciare le modalità di aggressione ad una condotta materiale dotata di un concreto disvalore penale, lesiva del bene individuale della *privacy* (a discapito di un bene poco afferrabile come quello della salvaguardia di

una c.d. estrinseca (accadimento da cui dipende solo l'opportunità di punire), cfr. Nuvolone, *Il diritto penale del fallimento e delle altre procedure concorsuali*, Milano, 1955, 14; Pagliaro (2003), p. 395, secondo cui le condizioni intrinseche sono "*veri e propri eventi mascherati*"; Bricola (2007), pp. 588. Per precisazioni critiche, cfr. Angioni (1989), pp. 1440; inoltre, Brunelli (2013), p. 80, sostiene che le condizioni intrinseche, in quanto elementi marginali, ma non estranei al fatto tipico, devono essere imputabili per colpa come "coefficiente soggettivo vicario conforme al principio di colpevolezza". Egli, peraltro, conclude censurando di infondatezza la distinzione tra condizioni obiettive di punibilità intrinseche ed estrinseche in quanto deve sostenersi la natura giuridica di evento del fatto di reato "giacché solo in tal modo non si tradisce la vera portata del canone costituzionale indotto dal principio di colpevolezza" (83). Si veda, infine, il Progetto Pagliaro (art. 13) che escludeva le condizioni obiettive intrinseche, atteso che veniva prescritto che le condizioni obiettive di punibilità dovessero essere estranee al piano dell'offesa tipica.

[52] Cfr. Corte Costituzionale n. 364/1988, con nota di Pulitanò (1988), p. 686.

[53] *Funditus* Angioni (1989), pp. 1440 s., secondo cui il principio di colpevolezza potrà considerarsi rispettato solo se le condizioni di punibilità siano coperte perlomeno dalla colpa in senso stretto; cfr. altresì Fiandaca e Musco (2012), p. 819; peraltro si erano espresse diffuse perplessità circa la legittimità costituzionale delle condizioni obiettive di punibilità c.d. intrinseche per violazione del principio di colpevolezza, cfr. Dolcini (2000), pp. 863, per il quale "soltanto gli elementi estranei alla materia del divieto (come le condizioni estrinseche di punibilità) si sottraggono alla regola della rimproverabilità *ex* art. 27, comma 1, Cost.".

[54] Così, Manna (2004), p. 22; Manna, Di Florio (2019), p. 897.

[55] Bricola (2007), p. 588.

[56] Cass. Pen., Sez. III, 9.7.2004, n. 30134. Ulteriori pronunce (Sez. III, 18 febbraio 2014, n. 7504; Sez. V, 14 ottobre 2009, n. 40078 e Sez. III, 15 giugno 2012, n. 23798) hanno ribadito l'orientamento per il quale si sarebbe in presenza di una condizione obiettiva di punibilità intrinseca e ciò essenzialmente perché il reato in questione (la cui condotta tipica consiste già nel trattamento illecito di dati personali) è già offensivo dell'interesse protetto a prescindere dall'effettivo nocumento. Secondo questa giurisprudenza, ritenere il nocumento come evento costitutivo del reato determinerebbe una notevole riduzione del campo applicativo della norma in quanto si dovrebbe necessariamente provare la presenza del dolo intenzionale; il nocumento – in carenza di una esplicita indicazione normativa – può riguardare anche soggetti terzi diversi da quelli titolari dell'interesse alla *privacy* oggetto di tutela penale.

[57] In giurisprudenza, la Corte di Cassazione (in part., Cass. Pen., Sez. III, 9.7.2004) ha escluso che la condizione obiettiva di punibilità possa essere integrata sia in presenza di mere irregolarità formali o procedimentali, quanto in presenza di "*inosservanze che producano un 'vulnus' minimo all'identità personale del soggetto ed alla sua privacy [...] sia nell'aspetto negativo sia positivo e non determinino alcun danno patrimoniale apprezzabile*". Si noti che nel caso di specie, si trattava della utilizzazione di dati personali ricavabili da un elenco di iscritti ad una associazione cui apparteneva lo stesso imputato per scopi elettorali e la Corte di Appello di Messina aveva ritenuto che tale condotta integrasse il reato di trattamento illecito dei dati personali per fini di propaganda politica, condannando l'imputato ex art. 35 L. 675/1996; la Corte di Cassazione ha, in seguito, annullato senza rinvio l'impugnata sentenza ritenendo fondate le doglianze del candidato alle elezioni comunali, ma solo perché nelle more del processo era entrata in vigore la normativa sopravvenuta di cui all'art. 167 Codice della privacy, che, come osservato, introduce la condizione obiettiva di punibilità del nocumento e che impone dunque un accertamento circa la derivazione di un apprezzabile *vulnus* alla persona offesa, non potendosi più sostenere la sussistenza di un reato di pericolo astratto o presunto; sul punto, si veda Palamara (2005), p. 1898.

A tal proposito, appare significativo il rapporto – anche per l'affinità degli interessi tutelati – che sussiste con il reato di rivelazione di segreti di ufficio di cui all'art. 326 c.p. (su cui anche nt. 17), il quale non richiederebbe, quale condizione di punibilità la sussistenza di un danno, ma la mera violazione dei doveri di ufficio: il reato *de quo* è stato, tuttavia, definito dalla giurisprudenza come reato di "*reato di pericolo effettivo e non meramente presunto nel senso che la rivelazione del segreto è punibile, non già in sé e per sé, ma in quanto suscettibile di produrre nocumento a mezzo della notizia da tenere segreta*", Cass. SS.UU., 27.10.2011, n. 4694.

mere funzioni del Garante), con l'obiettivo di superare in questo modo le censure di violazione del principio di legalità, pur sollevando contestualmente questioni di non poco momento sul piano del rispetto del principio di colpevolezza[58].

La condizione obiettiva di punibilità del nocumento si profilava dunque quale spartiacque del momento in cui la condotta – di per sé già illecita e lesiva degli interessi tutelati – assume quel carattere che legittima l'intervento del diritto penale. Infatti, con l'avverarsi della condizione, vi sarebbe – si afferma, non più solo *meritevolezza*, ma altresì – *bisogno di pena*[59], secondo una progressione criminosa sul piano dell'offesa, nel senso che la condotta violatrice del precetto extrapenale, a cui rinvia la norma incriminatrice, può essere punita con la sanzione penale – secondo una scelta di opportunità di natura politico-criminale – soltanto qualora dalla violazione *derivi*, quale conseguenza dell'azione, un *nocumento*: quest'ultimo quindi, a ben vedere, rivelerebbe la sua natura intrinseca rispetto al bene giuridico tutelato.

L'intervento riformatore – in questa occasione non imposto da alcun provvedimento comunitario – ha tentato di ricondurre il fuoco dell'incriminazione, attraverso il recupero dell'offensività del tipo delittuoso, subordinando la punibilità alla lesione del bene individuale della riservatezza e del controllo dei dati personali.

Sennonché, a ben vedere, l'intero sistema di tutela della *privacy*, costituito altresì da numerosi sanzioni di natura amministrativa[60], alcune delle quali costruite specularmente alla fattispecie di cui all'art. 167, ruota attorno all'istituzione di una nuova *Authority*, il c.d. Garante per la protezione dei dati personali, in qualità di autorità di controllo designata anche ai fini dell'attuazione del Codice della *privacy*[61].

In questo senso, può dunque giustificarsi la procedibilità d'ufficio del reato di trattamento illecito dei dati personali, unitamente agli altri illeciti penali, così da non lasciare alla disponibilità privata l'attivazione della giurisdizione penale. In questo schema di tutela sembrerebbe allora individuarsi una "*seriazione degli interessi da tutelare*"[62], in cui la protezione della vita privata del singolo è il "*bene strumentale*", mentre "*bene finale*" sarebbe proprio l'interesse alla sicurezza dei dati, ovvero all'efficientismo dell'ordinamento settoriale facente capo al Garante"[63].

Alla luce di dette considerazioni, la tecnica legislativa prescelta per la formulazione delle disposizioni penali, a ben vedere, all'interno dell'intero quadro normativo soffriva ancora di scarsa chiarezza ed intellegibilità, così da spingere verso una rivisitazione normativa che fosse adeguata alle moderne esigenze di tutela nel mondo dell'informatizzazione dei servizi e delle attività, secondo le linee riformatrici dettate dal Regolamento 2016/679/UE del Parlamento Europeo e del Consiglio del 27 aprile 2016 "*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*", che abroga la precedente Direttiva 95/46/CE.

[58] Sulla problematica coesistenza tra condizioni di punibilità intrinseche e principio di colpevolezza, altresì D'Ascola (1993), pp. 681, che, rifiutando una distinzione tra condizioni intrinseche ed estrinseche, sostiene che tutte le condizioni perseguono interessi estranei all'offesa tipica.

[59] M. Romano (1992), p. 39 s.; altresì, in questi termini, Manna (2004), p. 23. Cfr., in giurisprudenza, Cass. Pen., Sez. III, 17 febbraio 2011, n. 17215, Rv 249991, secondo cui "*il reato è perfetto quando la condotta si sostanzia in un trattamento dei dati personali, in violazione di precise disposizioni di legge, effettuato con il fine precipuo di trarne un profitto per sè o per altri o di recare ad altri un danno ma la sua punibilità discende dalla ricorrenza di un effettivo "nocumento" (nel senso, cioè, che il profitto conseguito o il danno causato siano apprezzabili sotto più punti di vista). Si è, in altri termini, al cospetto di un reato di pericolo effettivo e non meramente presunto [...], con il risultato che la illecita utilizzazione dei dati personali è punibile, non già in sè e per sè, ma in quanto suscettibile di produrre nocumento (cosa che, ovviamente, deve essere valutata caso per caso) alla persona dell'interessato e/o al suo patrimonio*". Cfr,, tuttavia sul punto Pagliaro (2003), p. 502, secondo cui la nozione dogmatica di perfezione del reato richiede l'integrazione di tutti gli elementi previsti per la rilevanza della condotta incriminata(dunque anche la condizione obiettiva di punibilità) e si distingue dalla consumazione che, invece, indica il momento in cui la realizzazione stessa raggiunge, nel suo contenuto concreto, la maggiore gravità. Sulla distinzione, invece, tra perfezione ed efficacia del reato, cfr. M. Gallo (1951), p. 24.

[60] In questa sede, seppur di notevole rilevanza, non ci sofferma sul problematico rapporto tra gli illeciti amministrativi e penali nella materia della *privacy*, per il quale si rinvia a Manes, Mazzacuva (2019), 176.

[61] Si può vedere il sito internet dedicato su: https://www.garanteprivacy.it . Si veda in letteratura, per tutti, per i profili più attuali di rilievo, Troncone (2011), p. 74 s.

[62] cfr. Fiorella (1990), p. 797.

[63] Cfr. ampiamente, *infra* par. 4.1. Si veda Manna (2004), p. 26 sosteneva, a tal proposito, che il "*mantenimento della procedibilità d'ufficio nelle ipotesi in esame, conferma, pertanto la natura anfibia di detti illeciti, in bilico tra la tutela di mere funzioni e la protezione di un assai più pregnante bene giuridico individuale*".

4. La nuova fattispecie di trattamento illecito dei dati personali

La riforma intervenuta con il GDPR – che viene indicato con l'acronimo "GDPR" (*General Data Protection Regulation*), entrato ufficialmente in vigore nell'area UE il 25 maggio 2018[64] – ha cristallizzato in modo definitivo la prevalenza dello strumento amministrativo, nell'ottica del doppio binario sanzionatorio, secondo gli auspici del legislatore europeo, attraverso "*l'imposizione di sanzioni penali per violazioni di […] norme nazionali e di sanzioni amministrative*", le quali, tuttavia, *"non dovrebbe essere in contrasto con il principio del* ne bis in idem *quale interpretato dalla Corte di giustizia*"[65], alla luce di un "*un sistema che preveda sanzioni effettive, proporzionate e dissuasive*"[66].

Il GDPR ha introdotto molte innovazioni – per lo più sconosciute anche ai più moderni ordinamenti giuridici occidentali nel campo della protezione dei dati personali – nel senso di una rimodulazione dell'intero sistema di controllo e gestione dei flussi di informazioni e dati all'interno del mondo digitale.

Tralasciando gli svariati aspetti di natura extrapenale[67] – e nell'ottica di valutare l'esito della trasposizione in Italia degli illeciti penali in materia[68] – va preliminarmente evidenziata l'anomalia di un Regolamento europeo che interviene con uno strumento di diretta applicazione nella materia penale, in apparente violazione dell'art. 83, par. 2 TFUE[69]. Infatti, l'art. 84 del GDPR prescrive l'adozione di sanzioni penali, auspicando altresì l'adozione di misure ablative[70], per le violazioni delle disposizioni tanto dello stesso regolamento quanto delle disposizioni nazionali da adottarsi in virtù di quest'ultimo, laddove, in linea generale, il diritto europeo imporrebbe l'adozione dello strumento legislativo della Direttiva – di applicazione solo mediata – per l'armonizzazione in materia penale[71].

È noto, d'altronde, che il potere legislativo in materia penale spetta agli Stati membri che si sono riservati la piena potestà punitiva: in tal senso, l'art. 83, par. 2 riconosce una competenza penale c.d. accessoria[72] all'UE solo per l'individuazione di "*norme minime relative alla definizione dei reati e delle sanzioni*", le quali "*possono essere stabilite [solo] tramite direttive*".

L'incompatibilità dello strumento prescelto, il regolamento, rispetto alla materia penale è stato solo in parte superato con la prescrizione di un ampio termine per la sua entrata in vigore, che potesse consentire agli Stati membri di adeguarsi e dotarsi degli strumenti necessari, secondo una modalità attuativa tipica delle Direttiva. In questo senso, si è ritenuto che il GDPR, quanto ai suoi effetti, si configuri come una "quasi direttiva"[73].

Orbene, in Italia, il legislatore delegato ha inteso dare attuazione al Regolamento europeo con il D. Lgs. 101/2018 recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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*". L'intervento legislativo incide notevolmente sullo schema normativo del Codice della Privacy attraverso la soppressione di numerose disposizioni e l'introduzione di nuove prescrizioni, in un quadro di tutela multilivello in cui l'elemento caratterizzante è costituito dall'eterointegrazione delle norme attraverso un espresso rinvio di cui all'art. 1 del Codice che sancisce che "*il trattamento dei dati personali avviene secondo le norme del regolamento (UE) 2016/679 e del presente codice, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona*".

[64] In generale, Pisapia (2018), in part. p. 119 s.
[65] GDPR, Considerando n. 49.
[66] GDPR, Considerando n. 152 e altresì Art. 84.
[67] Sui quali si rinvia ampiamente alle *guidelines* del Garante della Privacy, *Guida al nuovo regolamento europeo in materia di protezione dei dati personali*, 2016; in letteratura, tra gli altri, Pizzetti (2016); Bolognini *et al.* (2016).
[68] Si v. da ultimo l'opera di Manes, Mazzacuva (2019), p. 171 s. Sui profili di armonizzazione legislativa del Codice della *Privacy* in materia penale, si v. ampiamente D'Agostino (2019), in part. 29 ss.
[69] Art. 83, par. 2, Trattato sul Funzionamento dell'Unione Europea, dispone che "*allorché il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri in materia penale si rivela indispensabile per garantire l'attuazione efficace di una politica dell'Unione in un settore che è stato oggetto di misure di armonizzazione, norme minime relative alla definizione dei reati e delle sanzioni nel settore in questione possono essere stabilite tramite direttive*".
[70] Considerando n. 49 "*[…] Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento*".
[71] Come è avvenuto ad esempio in ipotesi di obbligo di incriminazione dei fatti di riciclaggio attraverso lo strumento della direttiva: l'ultima in ordine cronologico è la Quinta Direttiva Antiriciclaggio 2018/843.
[72] Bernardi (2012), p. 43 s.
[73] Cfr. Lamanuzzi (2017), p. 250.

In questo quadro, deve dunque inserirsi il tentativo di correggere gli errori di tecnica legislativa nella disciplina del reato di "*illecito trattamento dei dati personali*", in cui il legislatore segna il passaggio definitivo verso un'architettura penalistica volta ad una *tutela rafforzata* dell'intero sistema *privacy*, che assume definitivamente carattere pubblicistico, nonostante il disvalore di evento si appunti *strumentalmente* sul nocumento agli interessi di un privato[74].

L'art. 167 del Codice della privacy – recante "*Trattamento illecito dei dati personali*" – apre il Capo II del Codice dedicato agli "*Illeciti penali*" e sancisce che *"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"*[75].

Se, dunque, il cammino verso l'incriminazione del trattamento illecito dei dati personali sembrava essere segnato da un approccio legislativo in cui la punibilità è sottoposta ad una *doppia selezione* delle condotte meritevoli di sanzione, sia con riguardo all'aspetto subiettivo (con l'individuazione del dolo specifico[76]) che a quello oggettivo (con la previsione della condizione obiettiva di punibilità intrinseca), il legislatore del 2018 ha ulteriormente ristretto l'area del penalmente rilevante. Tale obiettivo è stato perseguito, per un verso, attraverso un'*abrogazione parziale* della norma, nella parte relativa alle condotte di trattamento poste in essere senza il consenso[77] e, per altro verso, attraverso una *tecnica legislativa* che sembra rimarcare,

[74] Cfr. Fiorella (1990), p. 797.

[75] A ben vedere, la norma – seppur rubricata trattamento illecito di dati personali – non fa più espresso riferimento alla modalità commissiva del *trattamento*, limitandosi a descrivere il precetto come mera *operazione* in violazione di una norma extrapenale. *Prima facie*, Si può notare che, per un verso, la fattispecie apparentemente ne beneficerebbe in termini di maggiore chiarezza, non dovendosi altresì accertare i tratti caratteristici del *trattamento dei dati personali*. Per altro verso, si noti che in precedenza era necessaria una condotta commissiva, secondo la descrizione (ora abrogata) dell'art. 4 lett. a) del Codice della privacy (nel senso che nel definire il concetto di "trattamento" l'art. 4 facesse riferimento a condotte attive, Troncone (2011), p. 132; Manna (2010), p. 779 ss.; Contaldo e Marotta (2004), p. 142 s.). Peraltro, a ben vedere, non sembra agevole individuare la ragione dell'espunzione dell'espressione del *trattamento dei dati* dalla formulazione del reato, che, al contempo, ne mantiene intatta la rubrica. Si potrebbe forse sostenere che la *ratio* del legislatore sia stata quella di contemplare anche l'ipotesi di commissione del reato attraverso una condotta omissiva: ad esempio, si pensi alla mancata cancellazione di un dato personale o mancata vigilanza nella trasmissione o gestione degli stessi. Sulla interpretazione giurisprudenziale della condotta di *trattamento*, si veda ad es. Cass. Pen., Sez. III, 16 maggio 2013, n. 29071, secondo cui "il reato di trattamento illecito di dati personali non è integrato se il trattamento dei dati avvenga per fini esclusivamente personali, senza una loro diffusione o destinazione ad una comunicazione sistematica" (ciò derivava, però, dalla clausola limitativa di cui all'art. 5, comma 3, secondo cui il trattamento di dati personali se 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", cfr. Celi (2010), p. 311).
La perplessità accresce ulteriormente laddove si volga lo sguardo al comma 2 dello stesso art. 167 che punisce con una pena più severa, ossia con la reclusione da uno a tre anni,"*chiunque, al fine di trarre per sé o per altri profitto, 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 ad esso relative ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quaterdecies arreca nocumento all'interessato*": nella fattispecie ora richiamata – e, si noti, sconosciuta alla formulazione precedente del reato – non solo permane l'espressione del trattamento dei dati personali, ma vi è un esplicito rinvio *per relationem* alle prescrizioni del GDPR che riguardano i c.d. dati particolari. Questi ultimi attengono all'origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, o appartenenza sindacale, nonché ai dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9), ovvero ai dati relativi alle condanne penali e reati (art. 10). In questi casi, tuttavia, si rafforza l'esigenza di tutela penale della *privacy*, nella sua accezione più propriamente individualistica volto alla tutela dei dati c.d. particolari.

[76] Nel senso di un dolo specifico "selezionatore", si veda meglio *infra*, par. 4.2.

[77] Ossia quelle previste dagli abrogati art. 23, ai sensi del quale "*il trattamento di dati personali da parte di privati o enti pubblici economici è ammesso solo con il consenso espresso dell'interessato*", e 24 "*Casi nei quali può essere effettuato il trattamento senza il consenso*". Siffatta *abrogatio* ripropone la questione della rilevanza del consenso nelle fattispecie di trattamento illecito dei dati personali. Nella precedente formulazione era, invero, pacifico che il consenso del titolare dei dati non si configurasse quale scriminante, ai sensi dell'art. 50 c.p., bensì quale *causa di esclusione delle tipicità del fatto*, ossia elemento negativo della fattispecie, nel senso che la sua assenza era elemento essenziale per l'integrazione del reato (Manna (2004), p. 29). Ora, nel novellato quadro normativo, le sole norme extrapenali a cui si fa rinvio sono l'art. 123 che riguarda i dati relativi al traffico; l'art. 126 sui ai dati relativi all'ubicazione e l'art. 130 relativo alle comunicazioni indesiderate. Le tre disposizioni richiamate – non di semplice lettura, in quanto constano di più commi e prescrizioni – consentono, *in linea di massima*, l'utilizzo dei relativi dati personali soltanto con il *consenso* del contraente o dell'utente. Il consenso, in questi casi, non avrebbe rilevanza scriminante, ma la sua assenza sarebbe elemento essenziale della fattispecie penale. Vi sono però prescrizioni la cui violazione non discende dalla mancanza del consenso, come ad esempio, il comma 1 dell'art. 123 in cui i dati relativi al traffico "*sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica*", che – all'evidenza – postulano una violazione tramite omissione (a prescindere dal consenso); o ancora, l'art. 130, comma 3-*bis*, secondo cui è consentito il trattamento dei dati nei confronti di chi non abbia esercitato il diritto di opposizione, postulando quindi la possibilità di trattamento dei dati a prescindere dal consenso e fintantoché non si abbia prestato il proprio *dissenso* (o si sia revocato il *consenso*, in questo caso da ritenersi implicito, cfr. Troncone (2011), p. 119 s.). Altro discorso, invece, deve essere sviluppato in relazione alla violazione del provvedimento del Garante di cui all'art. 129, relativo alle "*modalità di inserimento e di successivo utilizzo dei dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del pubblico*", le cui modalità di emissione sono specificamente illustrato dal comma 2 dello stesso articolo: si tratta di una vera e propria normale penale in bianco (cfr. Pagliaro (2003), p. 69, per il quale si ha legge penale in bianco quando la stessa faccia "*rinvio ad un atto normativo di grado inferiore per indicare tutti i contrassegni di un fatto che la legge medesima considera penalmente illecito*").

come si cerca di dimostrare nelle riflessioni che seguono, la stessa impostazione incriminatrice adottata nelle ipotesi in cui il diritto penale – per la tutela di interessi di natura generale – interviene nelle *situazioni di anomalia* nella regolamentazione delle relazioni ed affari tra privati, come avviene, tra le altre, in ipotesi di *patrocinio o consulenza infedele* di cui all'art. 380 c.p.

4.1. *Il* nocumento *come disvalore di evento.*

Nella fattispecie in analisi, la modifica di maggiore rilievo è certamente rappresentata dalla formulazione del *nocumento* in termini di *evento* – e dunque rientrante nella struttura tipica del *reato*[78] – e non più, come visto, di condizione obiettiva di punibilità intrinseca, che sebbene possa partecipare alla caratterizzazione offensiva del fatto incriminato, rimane pur sempre elemento futuro e incerto da cui dipende la punibilità dell'autore del reato.

L'effetto è quello di una ulteriore riduzione dell'area del penalmente rilevante, in quanto – abbandonando l'impostazione incriminatrice precedente che postulava un atteggiamento psicologico per cui era sufficiente la *prevedibilità* del *nocumento* – l'autore deve ora agire volendo e rappresentandosi il risultato dannoso.

Viene dunque costruito un reato di evento, che abbandona ora definitivamente l'impostazione formalistica originaria che subordinava la punibilità ad una mera condotta violatrice dei precetti extrapenali. L'evento di nocumento agli interessi dell'interessato deve essere, per l'appunto, conseguenza necessaria della dolosa violazione dei precetti extrapenali.

Nella riforma legislativa, a ben vedere, sembra confermarsi la strumentalità della sanzione penale per il contrasto al trattamento illecito dei dati personali. Il legislatore penale – pur perseguendo la tutela del bene individuale della riservatezza, consacrato ora altresì con l'inciso del *"nocumento all'interessato"*[79] – attraverso la minaccia della pena, intende, da un lato, presidiare l'interesse generale alla protezione dei dati personali e, dall'altro, salvaguardare le funzioni di controllo e gestione del Garante.

Non v'è chi non veda allora una strettissima affinità con il tipo delittuoso del *patrocinio o consulenza infedele*, che costruisce – in modo del tutto analogo – un reato di evento tutto incentrato sull'elemento del *nocumento agli interessi della parte*. Anche in questa ipotesi delittuosa, vi è il ricorso ad una tecnica legislativa che, punendo la condotta di un *patrocinatore* o *consulente tecnico*[80] trasgressiva di *doveri professionali*, ricollega l'offesa alla verificazione dell'evento del *nocumento agli interessi della parte*[81].

La collocazione sistematica del reato, all'interno del Libro II, Titolo III del codice penale relativo ai "*Delitti contro l'amministrazione della giustizia*", aveva fatto propendere dottrina e giurisprudenza verso la tutela di un'oggettività giuridica di natura pubblicistica, in cui si intende garantire la correttezza e lealtà da parte dei patrocinatori e consulenti tecnici per il regolare funzionamento dell'amministrazione giudiziaria[82]. A sostegno di questa impostazione, si è fatto ricorso, oltre alla collocazione sistematica, altresì alla Relazione ministeriale di accompagnamento secondo cui "*il concetto fondamentale […] è che si debbano reprimere gli abusi dei patrocinatori, considerati nei rapporti con l'amministrazione della giustizia, e solo indirettamente nei rapporti privati con i clienti*"[83].

Invero, a fronte di altri orientamenti dottrinali che, invece, privilegiano una prospettiva privatistica[84] vi è chi, escludendo altresì la natura di reato plurioffensivo, sostiene che la fattispecie sarebbe posta a tutela di un *unico interesse complesso*, individuato nell'interesse proces-

[78] Manes, Mazzacuva (2019), 172.
[79] Manes, Mazzacuva (2019), p. 173, in parziale difformità, secondo cui "le modifiche descritte possono essere giudicate positivamente poiché da un lato la maggiore centralità attribuita al nocumento per l'interessato risulta coerente con una logica di tutela personalistica e, dall'altro, la limitazione dei rinvii ad altre disposizioni attenua i noti problemi di indeterminatezza delle fattispecie in parola".
[80] Cfr. Art. 380 c.p. Si noti, peraltro, che la fattispecie *de qua* costruisce un reato proprio, non dissimilmente da quanto previsto dall'art. 167 Codice Privacy che – a dispetto del riferimento a "*chiunque*" – può essere commesso soltanto dal titolare o dal responsabile del trattamento o da colui il quale è stato da essi autorizzato al trattamento, sul punto cfr. Troncone (2011), p. 109.
[81] Si avverte che in precedenza la giurisprudenza considerava sufficiente qualunque azione od omissione idonea a procurare nocumento agli interessi della parte, secondo una ricostruzione in termini di condizione obiettiva di punibilità, cfr. Cass. Pen., 5 dicembre 1975, in *Riv. Pen.*, 1976, 860. Oggi, tuttavia, dottrina e giurisprudenza sono concordi nel considerare il nocumento quale evento tipico del reato, cfr. Calcagno (2009), p. 276.
[82] Calcagno (2009), p. 276.
[83] Si veda Catenacci *et at.* (2011), p. 552. Cfr. altresì, Fornasari (2017), p. 256.
[84] Fiandaca e Musco (2012a), 418.

sualpenalistico che ricomprende sia quello dell'amministrazione della giustizia sia al contempo quello della parte[85] . Secondo questa impostazione, il privato verrebbe in considerazione solo in quanto parte, ovvero in stretto rapporto con l'amministrazione della giustizia; giacché, ove gli interessi del privato non siano lesi e nemmeno posti in pericolo, non si realizza nemmeno l'offesa all'amministrazione della giustizia: "*Intanto l'amministrazione della giustizia può subire offesa, in quanto sia offesa la parte; e, viceversa, il privato può subire offesa come parte solo in quanto sia lesa o posta in pericolo la corretta amministrazione della giustizia*"[86].

Sicché, appurata la piena sovrapponibilità della struttura tipica tra il reato di trattamento illecito dei dati personali ed il reato di patrocinio o consulenza infedele, l'offesa penalmente rilevante – pur ponendosi in diretta relazione con il privato, titolare del bene individuale – emerge, per converso, solo in quanto sia leso o posto in pericolo l'intero sistema di protezione della *Privacy*, regolato dal Codice e sottoposto alla vigilanza del Garante[87]. Con la conseguenza che, anche nel tipo delittuoso *de quo*, sarebbe possibile individuare un *unico interesse complesso*, individuabile nell'interesse collettivo alla protezione dei dati personali, che è leso o posto in pericolo solo "*in quanto sia offesa la parte*".

Tale assunto, a tacer d'altro, trova definitiva conferma nella previsione – in entrambe le fattispecie criminose – della procedibilità d'ufficio, sicché, nonostante l'evento tipico di danno è ancorato ad un *pregiudizio privato*, all'evidenza la promovibilità dell'azione non è lasciata all'arbitrio della parte offesa, e dunque alla sua disponibilità.

4.2. *Il concetto di* nocumento *al vaglio della giurisprudenza*

L'individuazione del significato da attribuire all'espressione del *nocumento* ha peraltro impegnato la giurisprudenza, che ha tentato di tracciare i confini dell'offensività della condotta di trattamento illecito dei dati personali, distinguendolo anche dal concetto di danno.

È noto, d'altronde, a tal proposito, che per "danno" (anche in senso lessicale) si deve intendere ogni fatto circostanza o azione che "nuoce", sia materialmente che moralmente, e che la parola "nocumento" altro non significa (nella lingua italiana, con chiara derivazione latina) che "atto, o effetto, del nuocere": ne discende la quasi sovrapponibilità dei significati di tali parole[88].

Tuttavia, il significato dunque da attribuire alle due entità deve andare oltre la loro lettera e deve indurre a cercare il senso retrostante nella *ratio* posta alla base del suo inserimento nella fattispecie criminosa di cui si discute.

Già l'introduzione del "nocumento" nella novella legislativa del 2003, sembrava finalizzata ad evitare che la disposizione trovi un'applicazione eccessivamente formale e, quindi, come visto, aveva innanzitutto la funzione di dare "effettività" alla tutela della riservatezza dei dati personali[89].

L'accertamento della sussistenza del nocumento si risolve dunque in una *questio facti*. Innanzitutto, è necessario fissare il *quantum* del nocumento: in alcune pronunce di legittimità viene richiesto, ai fini dell'integrazione del reato secondo la formulazione precedente, che la condotta cagioni un *vulnus minimo all'identità personale del soggetto passivo e alla sua privacy*, in altre si fa riferimento a un *vulnus significativo alla persona offesa*[90].

Così, in un caso di propalazione da parte dell'indagato di informazioni relative alla vita sessuale della persona offesa alla sua nuova compagna, la Suprema Corte ha accertato la verificazione di un nocumento, costituito dal pregiudizio, anche di natura *non patrimoniale* subito

[85] Pagliaro (2003a), p. 178.
[86] Pagliaro (2003a), p. 178.
[87] In relazione al *disvalore di evento* ed alla possibilità di individuare un bene giuridico ultimo ed un bene giuridico prossimo, secondo uno schema di c.d. *seriazione dei beni giuridici*, cfr. Fiorella (1990), p. 797.
[88] Così si esprime la giurisprudenza, per tutte, Cass. Pen., Sez. III, 17 febbraio 2011, n. 17215, Rv 249991.
[89] In tal senso, non è utile sforzarsi nella ricerca di un *discrimen* tra le due parole che non riguardi direttamente la direzione teleologica della disposizione in esame; non appare utile dilungarsi in affannosi tentativi di differenziazione terminologica, per cui il danno sarebbe l'evento naturalistico collegato alla condotta tipica ex art. 40 c.p. ed il nocumento riguarderebbe l'insieme delle conseguenze negative in senso lato, quali, ad esempio, le ripercussioni sgradevoli e disonorevoli che dal fatto possono derivare anche a persone diverse dal soggetto passivo (cfr. Troncone (2011), p. 159); tale prospettazione è, peraltro, ancor meno veritiera adesso alla luce della costruzione del reato con un evento di danno, secondo l'espressione del *nocumento all'interessato*.
[90] Si noti, a tal proposito, che si era profilato un filone giurisprudenziale che – nella vigenza della precedente formulazione – aveva ritenuto che il nocumento "*non è soltanto quello derivato alla persona fisica o giuridica cui si riferiscono i dati, ma anche quello causato a soggetti terzi quale conseguenza dell'illecito trattamento*" (cfr. Cass. Pen., Sez. III, 16 luglio 2013, n. 7504), giacché, sotto questo profilo, si è avuta una *abolitio criminis*, attesa ormai la specificazione del "nocumento all'interessato

dalla persona cui si riferiscono i dati quale conseguenza dell'illecito trattamento[91]. Per converso, in un altro caso, veniva ritenuta l'assenza di nocumento per il fatto di due soci di un'associazione che, senza autorizzazione, avevano pubblicato l'immagine di un altro socio dell'opuscolo della medesima associazione, non avendo individuato alcuna conseguenza pregiudizievole[92]. L'indagine del giudice, non potendosi trovare *ex ante* un sicuro parametro cui riferirsi, deve avere riguardo a tutte le circostanze del caso concreto, come si evince, in altra pronuncia di merito, in cui l'imputato è stato condannato per avere pubblicato, senza il preventivo consenso degli aventi diritto, un necrologio su un sito internet dallo stesso gestito, sull'assunto secondo cui il concetto di nocumento ricomprenderebbe "*tutte quelle forme di fastidio e turbamento subito dalla persona offesa, senza che sia necessario dimostrare una vera e propria lesione di un diritto autonomo e diverso rispetto al diritto di controllare l'uso che si fa dei propri dati personali*"[93]; ovvero ancora in una pronuncia di legittimità si arriva ad accertare la sussistenza di un *nocumento* anche nella "*perdita di tempo nel vagliare mail indesiderate e nelle procedure da seguire per evitare ulteriori invii*"[94]

In definitiva, la giurisprudenza – come visto, onerata del compito di dare concretezza al *Tatbestand* – ha dovuto scontare un disagio di disarmonia concettuale con cui sono stati utilizzati e collocati i requisiti strutturali della fattispecie, con la conseguenza di dovere individuare una autonoma funzione del danno e del nocumento. A tal proposito, i giudici hanno quindi tentato di offrire a ciascuno un preciso contenuto oggettivo di valore e una differente *ratio*: ciononostante, la coesistenza dei due concetti solleva profili problematici altresì sul piano soggettivo, come si cerca di illustrare di seguito.

4.3. *Un caso (unico) di dolo specifico apparente.*

La fattispecie in esame richiede, innanzitutto, la sussistenza del *dolo generico*, nel senso che il soggetto agente deve "*operare*" con un atteggiamento volitivo ed intellettivo tale da volere e prevedere[95] gli elementi di tipicità[96] e dunque tanto la violazione delle disposizioni extrapenali a cui si fa rinvio[97], quanto il *nocumento all'interessato*. In questo senso, il tipo delittuoso *de quo* richiede la coincidenza tra ciò che materialmente si realizza (c.d. *Erfolg*) e ciò che si riflette nella sfera intellettiva e volitiva dell'agente, giacché l'agente deve volere e rappresentarsi – nei limiti tracciati dalla rilevanza giuridica e nei termini descritti dagli elementi del reato – che la sua azione comporti un accadimento esteriore tale da arrecare *nocumento* alla persona titolare dei dati oggetto del trattamento[98].

Oltre al requisito del dolo generico, la formulazione del reato mantiene il dolo specifico, in quanto l'agente deve operare "*al fine di trarre profitto o di arrecare un danno*". Come noto, il dolo in questione deve indicare una volontà ulteriore e diversa rispetto agli elementi di tipicità, nel senso che deve rivolgersi ad una finalità la cui realizzazione non è necessaria ai fini della punibilità e dunque dell'integrazione del fatto di reato. Viene usualmente indicato come *mera intenzione* del soggetto, senza che al contempo risulti violato il principio di materialità del fatto tipico.

Si distinguono usualmente alcune tipologie di dolo specifico, che non è possibile in questa

[91] Cass. Pen., Sez. III, 7 febbraio 2017, n. 29549.
[92] Peraltro, nella stessa pronuncia, si afferma che "*il concetto di nocumento alla persona deve ritenersi ben più ampio di quella di danno comprendendo, qualsiasi effetto pregiudizievole che possa conseguire alla arbitratia condotta invasiva altrui*", Trib. Bari, 3 marzo 2016, n. 327.
[93] Trib. Perugia, 26 giugno 2015, n. 1100.
[94] Nel caso di specie, la Cassazione ha condannato l'amministratore delegato ed il direttore finanziario di una società a cui era stata contestata l'attività di spamming con invio di una newsletter a soggetti che non l'avevano richiesta e che al contempo inviavano mail di protesta al gestore del *database*, Cass. Sez. III, 24 maggio 2012, n. 23798.
[95] Cfr. Pagliaro (2003), p. 278.
[96] Cfr. in tal senso Fiandaca e Musco (2012), p. 373, secondo cui l'art. 47 c.p., stabilendo che il dolo è escluso dall'errore sul fatto che costituisce il reato, implicherebbe che la rappresentazione e la volontà devono avere ad oggetto il "fatto tipico".
[97] Sul punto, è bene precisare che il dolo, nel suo aspetto volitivo e rappresentativo, riguarda il significato assunto dall'elemento normativo nel linguaggio del profano, che consente all'agente di percepire la lesività del proprio comportamento; con la conseguenza che, in ipotesi di qualificazioni extrapenali, non se ne pretende la meticolosa conoscenza del giurista, ma ci si accontenta della approssimativa parallela conoscenza profana; tra gli altri, Brunelli, *Il diritto delle fattispecie criminose*, Torino, 2013, 101.
[98] Nel senso che oggetto del dolo è l'evento significativo, ossia "l'accadere esteriore nel suo significato umano e sociale", Pagliaro (2003), p. 293; in senso conforme, ma facendo riferimento al "fatto tipico", quale oggetto del dolo, cfr. Fiandaca e Musco (2012), p. 373; nel senso, invece, che oggetto del dolo sarebbe l'"evento giuridico", ossia l'offesa all'interesse protetto dalla norma, Delitala (1930), p. 64; nel senso, infine, dell'oggetto del dolo quale "evento naturalistico", cfr. Antolisei (1928).

sede ripercorrere[99]. Giova, peraltro, evidenziare come ad esso si faccia principalmente ricorso in ipotesi di c.d. "*dolo specifico selettivo o differenziatore*", che si ha qualora il fatto risulti già sufficientemente descritto quanto a modalità oggettive, sicché, essendo la condotta oggettiva già offensiva del bene protetto, la finalità *ulteriore* non arreca un contributo nuovo o particolarmente significativo al contenuto dell'offesa[100].

Orbene, il ricorso al dolo specifico era stato inteso originariamente proprio nel senso di selezionare le condotte realmente offensive del bene giuridico tutelato dalla norma *de qua* onde evitare un eccessivo ampliamento dell'area del penalmente rilevante. In effetti, nella costruzione di una fattispecie incriminatrice fondata su elementi meramente *formalistici*, ossia sulla violazione di norme *extrapenali*, il dolo specifico svolgeva il ruolo selettivo delle condotte suscettibili di sanzione penale: in tal senso, soltanto una violazione del Codice della *privacy* che fosse determinata da una *finalità di lucro o di danno* legittimava l'intervento penalistico.

La modifica della struttura del reato che oggi prevede quale *evento* (su cui si appunta il contenuto lesivo ed è dunque, nei profili visti *supra*, oggetto del dolo) la sussistenza del nocumento all'interessato – che configura il tipo quale reato di danno – appare incompatibile con il mantenimento del dolo specifico in funzione di selezione delle violazioni delle prescrizioni richiamate in materia di *privacy*.

Nel caso di specie, la finalità ulteriore perseguita dal soggetto si sovrappone al risultato materiale (*Erfolg*), ossia all'evento naturalistico ed al contenuto offensivo del reato. Si tratta, a ben vedere, di un *dolo specifico di danno apparente*: sarebbe, quantomeno *prima facie*, del tutto superfluo in quanto la finalità o partecipa alla struttura della tipicità, e dunque è necessaria la sua realizzazione esteriore, ovvero è soltanto ulteriore rispetto alla struttura tipica del fatto, con la conseguenza che – nell'esercizio della sua funzione selettiva – individua tra le finalità dell'agente quelle lesive del bene tutelato. Dunque, delle due l'una: la finalità di danno è oggetto del dolo o è ulteriore rispetto alla struttura tipica.

Peraltro, a ben vedere, non risultano, all'interno del sistema penale integrato, altri tipi delittuosi costruiti nei termini qui formulati. L'unico esempio di tal fatta si rinviene nel precedente Codice Zanardelli che nella definizione dell'omicidio doloso conteneva l'inciso "*al fine di uccidere*". Detta formulazione fu tacciata di superficialità tanto da essere soppressa nel progetto preliminare del Codice Rocco, siccome incompatibile con le norme generali sull'elemento soggettivo del reato contenute nel libro primo (II comma dell'art. 42 e 43, prima parte). Anche in quell'ipotesi, si sarebbe potuto parlare di *dolo specifico apparente*, nonostante fosse plausibile una doppia selezione, tanto sul piano oggettivo – con l'accertamento dell'evento infausto – quanto sul piano soggettivo, attraverso la partecipazione della finalità al contenuto offensivo del fatto; e ciò al fine di differenziare l'omicidio doloso dall'ipotesi delittuosa meno grave dell'omicidio preterintenzionale[101].

Orbene, ritornando alla fattispecie qui in esame, è doveroso chiedersi se permanga una – seppure marginale – utilità del dolo di danno, nella sua funzione selettiva delle condotte suscettibili di sanzione penale: d'altronde, appare difficile pensare ad un trattamento illecito dei dati personali che, arrecando un *nocumento*, non sia accompagnato da una tale finalità.

A ben vedere, la formulazione normativa è il frutto di un *iter* legislativo che – nella bozza preliminare – non prevedeva più il dolo di danno, il quale avrebbe lasciato il posto soltanto al dolo specifico di profitto, con una ulteriore riduzione dell'area del penalmente rilevante.

Notevoli e fondate apparivano dunque le critiche rivolte allo *schema di decreto*: meno ragionevole, tuttavia, è stata la novellazione, per i motivi che seguono.

Da un lato, l'eliminazione delle fattispecie di danno e di violazioni non lucrative sembrava diminuire la tutela di fatti incresciosi come il *revenge porn* o lo *slut shaming*[102], che dovrebbero al contrario essere oggetto di attenta tutela.

A tal proposito, il Garante della Privacy europeo riteneva che la sola previsione del dolo specifico di profitto (vantaggio o altra utilità) fosse "*un'involuzione normativa, particolarmente*

[99] Sul tema, ampiamente, per tutti, Picotti (1993); nel senso che il dolo specifico non sia nemmeno una forma di dolo, perché estraneo alla condotta illecita, cfr. Pagliaro (2003), p. 287.

[100] Esempio classico di questa tipologia è la fattispecie del furto in cui il fine di trarre profitto dalla cosa mobile altrui svolge esclusivamente la funzione di selezionare le condotte punibili, dal momento che nella stessa condotta di sottrazione e impossessamento della cosa risulta già insito l'attacco al patrimonio; cfr. Brunelli (2013), p. 113.

[101] Sul punto, cfr. Mantovani (2016), p. 153.

[102] Si tratta di quei fenomeni, ormai molto diffusi, soprattutto tra i giovani, in cui avviene una condivisione online o tramite social di immagini o video intimi (aventi spesso sfondo sessuale) senza il consenso della o del protagonista degli stessi, come forma di vendetta o ritorsione, cfr. Citron e Franks (2014), p. 345.

inadeguata" in quanto "*non idonea ad inglobare al suo interno i fenomeni fortemente lesivi dei diritti alla personalità sorretti dalla coscienza e volontà di trattare dati personali al fine di danneggiare terzi soggetti*"[103]. Similmente, si esprimeva il Garante nazionale il quale propugnava l'inserimento del dolo alternativo di danno "*in ragione dell'esigenza di presidiare con la sanzione penale condotte connotate da un simile disvalore*", al fine peraltro "*di assicurare una maggiore continuità normativa con la fattispecie vigente e di evitare gli effetti (anche sui processi in corso) dell'abolitio criminis che si dovesse ravvisare, in parte qua, per effetto della novellazione proposta*"[104].

Dall'altro lato, nonostante la questione fosse stata correttamente individuata – ossia, la necessità di non lasciare impuniti fatti di grave allarme sociale, come il *revenge porn* o l'utilizzo di immagini e video con finalità di discredito, intimidazione o minaccia, come anche la necessità di assicurare la continuità normativa – la soluzione proposta è stata erroneamente impostata.

Se è vero che il dolo specifico *aggiunge* una finalità ulteriore ai caratteri della fattispecie delittuosa, che ben può sussistere soltanto interiormente nella psiche dell'agente, è altrettanto vero che la nuova formulazione impone una sua manifestazione esteriore, attraverso l'espressione del *nocumento all'interessato*: non solo il soggetto deve agire con siffatta *intenzione di danno*, ma deve ottenere materialmente il risultato (*Erfolg*): si disperderebbe, invero, la funzione selettiva del dolo specifico di danno.

Se, davvero, dunque, si fosse voluto perseguire con efficacia i fatti di maggiore allarme sociale – che il *web* rende ancora più insidiosi – sarebbe stato forse più opportuno espungere del tutto il dolo specifico, tanto di danno quanto di profitto.

Tale soluzione non avrebbe certamente tradito neppure l'auspicio del legislatore di circoscrivere l'area del penalmente rilevante, giacché l'elevazione dell'elemento del *nocumento* ad evento del reato, coperto dal fuoco del dolo, senza alcuna selezione delle condotte sorrette dal dolo specifico di profitto e di danno, eviterebbe, per un verso, l'incongruità[105] di una duplicità della finalità di danno e, per altro, garantirebbe comunque la continuità normativa. In quest'ultimo senso, si eviterebbe altresì, a ben vedere, la temuta *abolitio criminis*, in quanto sussisterebbe ancora un'analogia strutturale del reato *pre* e *post* riforma, atteso che identici sarebbero gli elementi materiali e che, venendo meno *in toto* la funzione selettiva del dolo specifico, si riespanderebbe, piuttosto che ridursi, l'area del penalmente rilevante[106].

Il legislatore ha, ciononostante, mantenuto entrambe le forme di dolo specifico.

Ne discenderebbe peraltro, a ben vedere, il pericolo di una *interpretatio abrogans* del *dolo specifico di danno*. Onde evitare siffatto esito, una soluzione ermeneutica di 'compromesso' – nell'ottica di attribuire un significato all'intenzione del legislatore, secondo una interpretazione teleologica – potrebbe forse prendere spunto da quanto avveniva con l'omicidio volontario sotto la vigenza del Codice Zanardelli[107]: il *dolo di danno* avrebbe dunque l'effetto di configurare il reato come reato a dolo intenzionale (e non specifico), qualificazione che si identifica nella direzione della volontà alla verificazione dell'evento, che si realizza secondo l'intenzione; pertanto, la previsione del dolo di danno renderebbe inapplicabile il reato di trattamento illecito quando la condotta sia sorretta da un dolo eventuale ovvero indeterminato[108].

La conseguenza è allora quella di una – inconsapevole – restrizione dell'area del penalmente rilevante adesso verificatasi sul versante soggettivo, il che in definitiva finirebbe col frustrare le esigenze di tutela prospettate dal Garante.

E a ben vedere, infine, se davvero la *ratio legis* fosse stata quella di tutelare il bene giuridico individuale della riservatezza, il reato di cui all'art. 167 sembra divergere dagli altri modelli delittuosi in cui il legislatore tutela la sfera privata senza subordinare la punibilità ad un dolo specifico di danno. Basti pensare, a titolo esemplificativo, alla ipotesi di cui all'art. 620 c.p., in cui si punisce la *Rivelazione del contenuto di corrispondenza, commessa da persona addetta al servizio delle poste, dei telegrafi o dei telefoni*, che è reato di mera condotta di rivelazione, senza alcuna selezione delle intenzioni criminose; ovvero al reato di *Rivelazione del contenuto di documenti segreti* di cui all'art. 621 c.p., in cui – premessa la punibilità per la mera condotta di

[103] Le opinioni del Garante *Privacy* europeo allo schema del decreto si possono visualizzare sul sito web https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9163359

[104] Cfr. sulle opinioni del Garante *Privacy* italiano allo schema del decreto, vedi altresì nt. precedente.

[105] Cfr. Manna (2004), p. 22. Cfr. *supra* par. 3.

[106] Cfr. Cass. SS.UU., 16 giugno 2003, n. 25888, Rv. 224607.

[107] Ramacci (2016), p. 43.

[108] Manes, Mazzacuva (2019), 173, secondo cui "la finalità dell'agente, coincidendo con l'oggetto del dolo generico, dif fatto lo qualifica come *intenzionale*". Inoltre, possono rinvenirsi simili riflessioni con riguardo ai reati tributari con dolo specifico, per i quali, si veda, per tutti, Salcuni (2001), p. 131 s.

rivelazione – viene aggiunta una ipotesi di impiego subordinata, tuttavia, ad un dolo specifico "*a proprio o altrui profitto*" e alla condizione obiettiva di punibilità del *nocumento*.

5. Il nuovo fuoco della tutela penale del trattamento illecito dei dati personali

Proseguendo nell'analisi della complessa formulazione della tutela penale in materia, ci si avvede che il vero fuoco di essa si rinviene ora in due nuovi tipi delittuosi introdotti da ultimo agli art. 167-*bis* "*Comunicazione e diffusione illecita di dati personali riferibili a un rilevante numero di persone*" e 167-*ter* "*Acquisizione fraudolenta di dati personali*"[109]. Di una tale rilevanza delle figure menzionate è indicatore la relativa previsione di un trattamento sanzionatorio più severo rispetto alla fattispecie base dell'art. 167 del Codice *privacy*[110].

L'art. 167-*bis* punisce due condotte materiali che sono definite dal nuovo art. 2-*ter* del Codice, ossia la *comunicazione* e la *diffusione*. Queste due modalità di manifestazione differiscono soltanto con riguardo ai soggetti destinatari, che astrattamente verrebbero a conoscenza dei dati personali: mentre nella comunicazione i destinatari sono determinati, al contrario nel caso della diffusione i destinatari sono invece indeterminati[111]. Elemento essenziale della nuova fattispecie di reato è che la condotta si riferisca ad un "*archivio automatizzato o a una parte sostanziale di esso contenente dei dati personali oggetto di trattamento su larga scala*".

In questa espressione viene, innanzitutto, evocato per la prima volta quale oggetto del reato un "*archivio automatizzato*", del quale però non si rinviene alcuna definizione nel Codice della Privacy. A ben vedere, il termine rimanda ad una nozione di natura informatica e digitale, la cui effettiva comprensione richiede avanzate conoscenze tecniche. L'art. 4, n. 6 del GDPR definisce un "*archivio*" come "*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*". In attesa di una elaborazione giurisprudenziale in proposito, si può sostenere che l'attributo "automatizzato" faccia riferimento ad un insieme di dati la cui elaborazione e gestione sia sottoposta ad automatismi computazionali svincolati da un diretto ed immediato coinvolgimento di una persona fisica.

In via esemplificativa, si potrebbe pensare al noto fenomeno della c.d. *profilazione*, che emerge anche normativamente dall'art. 22 del GDPR, secondo cui "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*"

Da questo punto di vista, si comprenderebbe l'altra espressione – anch'essa sconosciuta nel panorama penalistico – del "*trattamento su larga scala*", che, ad ogni buon conto, solleva evidenti questioni di tassatività del precetto penale secondo una tecnica legislativa che ricalca i paradigmi di una legislazione simbolica ed emergenziale. In definitiva, vengono lasciati ampi margini di discrezionalità all'opera ermeneutica del giudice, al quale viene demandato l'onere di provvedere alla sua efficienza pratica, colmando l'indeterminatezza e genericità dell'espressione del "*trattamento su larga scala*"[112]. Spetterà, dunque, al giudice individuare il momento in cui avviene la lesione al bene giuridico tutelato – che legittima l'intervento della sanzione penale – ed individuabile, nel caso di specie, nel diritto dei *consociati* ossia della collettività (e non più del singolo o, meglio, del diretto "interessato") al corretto utilizzo dei dati personali, con particolare riguardo ai sistemi informatizzati e automatizzati.

Peraltro, non appare peregrino evidenziare che l'espressione *de qua* è anch'essa frutto di un *iter* legislativo complesso, tanto perché si inserisce all'interno del sistema di tutela multilivello del GDPR e dell'eterointegrazione normativa in materia, quanto perché il reato di nuovo

[109] Cfr. per un primo commento sulle nuove disposizioni penali altresì, D'Agostino (2019), in part. 42 ss.
[110] L'art. 167-*bis* prevede la pena della reclusione da uno a sei anni, mentre l'art. 167-*ter* prevedono la pena della reclusione da uno a quattro anni.
[111] Si tenga presente, peraltro, che le due espressioni erano già presenti nella fattispecie base dell'art. 167 ("*se il fatto consiste nella comunicazione o diffusione*"). A tal proposito, in dottrina, si riteneva che – vigente la precedente formulazione – per punire la comunicazione e diffusione non occorresse la derivazione del nocumento, in quanto la mancata previsione normativa faceva suppore che il potenziale diffusivo della divulgazione del dato o dei dati sia di per sé solo sufficiente a garantire la punibilità del fatto, senza la concretizzazione della condizione di un effettivo danno, cfr. Manna (2005), p. 257.
[112] Cfr. Resta (2019), p. 1037.

conio, nell'*intentio legis* di colpire condotte di recente emersione[113], è il risultato di rilevanti emendamenti. Originariamente, la condotta lesiva era descritta attraverso il ricorso ad espressioni di altrettanta indeterminatezza, laddove il momento dell'offesa si sarebbe verificato qualora il trattamento si fosse riferito "*ad un rilevante numero di persone*".

A seguito di opinioni dissenzienti da parte del Garante della Privacy[114], sia italiano che europeo, si è tentato di individuare un criterio che non facesse solo leva sul criterio quantitativo, ma avesse anche una qualche valenza qualitativa. La scelta incriminatrice, tuttavia, ha mantenuto il riferimento ad una nozione di natura quantitativa: a ben vedere, non sussisterebbe alcuna differenza sostanziale tra un "*rilevante numero di persone*" ed "*un trattamento su larga* scala". Sarebbe stato senz'altro più coerente con l'intero sistema di tutela qualificare la condotta in termini invece qualitativi, nel senso di collegarla alla comunicazione o diffusione di dati personali c.d. particolari, ossia giudiziari e sensibili (di cui all'art. 2-*sexies*).

Sulla fattispecie *de qua* grava dunque un'ipoteca di illegittimità costituzionale per violazione del principio di tassatività e sufficiente determinatezza del precetto, quale corollario del principio di legalità.

Come anticipato, l'altra nuova incriminazione – che, nel sistema di tutela integrato, rende ulteriormente marginale la fattispecie base del trattamento illecito dei dati personali – è costituito dal nuovo art. 167-*ter* che, "*salvo che il fatto non costituisce più grave reato*" punisce con la reclusione da uno a quattro anni "*chiunque, al fine trarne profitto per sé o altri ovvero di arrecare un danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala*".

Anche in questa ipotesi delittuosa permane un dolo specifico di profitto e danno, in funzione selettiva delle condotte realmente offensive, ma al contempo viene formulato un reato di mera condotta, consistente nell'acquisizione fraudolenta, che è già perfetto a prescindere dall'accertamento di un nocumento. Da questo punto di vista, anche in questo tipo delittuoso, la tutela dal bene-categoria individuale della *privacy* non rileva ai fini della punibilità, se non nei limiti in cui viene riproposto un dolo specifico di danno, il quale, tuttavia, come noto, non deve verificarsi ai fini dell'integrazione del reato. La *ratio* dell'incriminazione si può allora rintracciare nell'interesse generale dei consociati ad una tutela rafforzata dei sistemi automatizzati, il cui utilizzo fraudolento deve essere presidiato da una sanzione penale.

Le due fattispecie delittuose si allontanano definitivamente dai profili privatistici ed individualistici del bene-categoria della *privacy*, che rimane soltanto sullo sfondo e la cui offesa non rileva neppure in termini di tipicità, come nell'ipotesi base dell'art. 167, secondo la struttura di reato di danno. Ebbene, in altri termini, nell'ottica di massima efficienza del nuovo modello di protezione dei dati personali auspicato dal legislatore europeo, il disvalore penale non risiede più nella lesione di un bene individuale, che può ben concretizzarsi nell'accertamento del *nocumento all'interessato*.

Invero, la lesione è rivolta ad una nuova e più pregnante oggettività giuridica – prima sconosciuta, e di nuova emersione alla luce dei nuovi utilizzi dei mezzi informatici e digitali – inquadrabile nell'*interesse generale dei consociati al corretto utilizzo delle piattaforme digitali, contenitori automatizzati di innumerevoli dati personali*: queste ultime – nell'ottica di una maggiore efficienza del sistema integrato di tutela – necessitano di un controllo giuridico più stringente, che può giungere anche all'inflizione della sanzione penale.

Il ragionamento dunque appare conforme agli auspici del legislatore europeo che ha imposto agli Stati membri di fare ampio ricorso alla sanzione amministrativa, la quale, nel rispetto del principio di sussidiarietà, deve cedere il posto a quella penale soltanto nelle ipotesi di maggiore allarme sociale. E sol che si ponga mente alle potenzialità lesive dei sistemi informatizzati e digitalizzati, ci si avvede della necessità di un presidio penale. In questo senso, la scelta incriminatrice sembra adeguata alla tutela del *sistema di protezione dei dati personali*, che assurge oggi – alla luce degli art. 167 s. Codice della Privacy – a nuovo bene-categoria di natura pubblicistica. Rimane tuttavia la perplessità di un ricorso ad elementi vaghi, come gli "*archivi automatizzati*" o ancora "*il trattamento su larga scala*", la cui concretizzazione spetterà all'attenta opera ermeneutica del giudice.

[113] Si pensi, tra gli altri, al celebre scandalo di *Cambridge Analytica*; cfr. *Carol Cadwalladr*, *The Cambridge Analytica file*, in *The Guardian*, 18 marzo 2018.
[114] Cfr. sul sito del Garante della privacy, cfr. *supra* nt. 103.

Bibliografia

Angioni, Francesco (1989), "Condizioni di punibilità e principio di colpevolezza", *Rivista Italiana di Diritto e Procedura Penale*, 1440 ss.

Angioni, Francesco (1994), *Il pericolo concreto come elemento della fattispecie penale: la struttura oggettiva* (Milano, Giuffrè).

Antolisei, Francesco (1928), *L'azione e l'evento nel reato* (Milano, Istituto Editoriale scientifico)

Antolisei, Francesco (2003) *Manuale di diritto penale. Parte Generale* (Milano, Giuffrè)

Bernardi, Alessandro (2012), *La competenza penale accessoria dell'Unione Europea: problemi e prospettive*, *Diritto penale contemporaneo – Rivista trimestrale*, 1, pp. 43 ss.

Bolognini, Luca, Pelino, Enrico, Bistolfi, Camilla (2016), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali* (Milano, Giuffrè).

Bricola, Franco (1967), *Prospettive e limiti della tutela penale della riservatezza*, *Riv. it. dir. proc. pen.*, pp. 1114 ss.

Bricola, Franco (2007), *Punibilità (condizione obiettive di)*, in *Noviss D.I.*, Torino, Giappichelli, 588 ss.

Brunelli, Ivan (2013), *Il diritto delle fattispecie criminose*, II Ed. (Torino, Giappichelli).

Calcagno, Elisabetta (2009), *Reati contro l'amministrazione della giustizia*, Vol. 7, (Giuffrè, Milano).

Canestrari, Stefano (1991) "Reato di pericolo", *Enc. Giur. Treccani*, XXVI, pp. 7 ss.

Carnelutti, Francesco (1955) "Diritto alla vita privata (Contributo alla teoria della libertà di stampa)", *Riv. trim. dir. pubbl.*, 4, 3 ss.

Catenacci, Mauro *et al.* (2011), *Reati contro la pubblica amministrazione e contro l'amministrazione della giustizia*, in *Trattato teorico-pratico di diritto penale*, diretto da Palazzo, Francesco, Paliero, Carlo Enrico (Torino, Giappichelli).

Celi, Loredana (2010), "Il ruolo del limite espresso dall'art. 5, comma 3, del d.lg. n. 196/2003 nella struttura del delitto di trattamento illecito di dati personali", *Cass. Pen.*, 1, pp. 311-319.

Citron, Danielle Kitts, Franks, Mary Anne (2014), "Criminalizing revenge porn", *Wake Forest Law Review*, 49, pp. 345 ss.

Contaldo, Alfonso, Marotta, Egidio (2004), "Depenalizzazione e nuove tutele dei dati personali anche alla luce del Codice della Privacy (d.lgs. 30 giugno 2003, n. 196)", *Giur. merito*, pp. 142 ss.

Corrias Lucente, (1997), "Sanzioni penali e amministrative a tutto campo per aumentare la tutela del cittadino", *Guida dir.*, 4, pp. 82.

D'Agostino, Luca (2019), "La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101", *Archivio Penale*, fasc. 1.

D'Ascola, Vincenzo Nico (1993), "Punti fermi i aspetti problematici delle condizioni obiettive di punibilità", *Rivista Italiana di Diritto e Procedura Penale*, pp. 652-681.

Delitala, Giacomo (1930), *Il fatto nella teoria generale del reato* (Padova, Cedam).

Dolcini, Emilio (2000): "Responsabilità oggettiva e principio di colpevolezza", *Rivista italiana di diritto e procedura penale*, pp. 863-882.

Fiandaca, Giovanni, Musco (2012), *Diritto penale. Parte Speciale*, Vol. I, V ed. (Milano, Giuffrè)

Fiore, Stefano (1999), voce *Riservatezza (diritto alla)*, IV, *Enc. giur. Treccani*, Roma.

Fiorella, Antonio (1990) voce *Reato. Il reato in generale (diritto penale)*, in *Enc. Dir.*, XLII, pp. 770-816.

Fornasari, Gabriele (2017), "Patrocinio o consulenza infedele", in Fornasari, Gabriele, Riondato, Silvio (a cura di), *Reati contro l'amministrazione della giustizia* (Torino, Giappichelli), pp. 256 ss.

Galdieri, Paolo (2012), "Il trattamento illecito del dato personale nei social network", *Giur. mer.*, 12, pp. 2697.

Gallo, Marcello, *Il concetto unitario di colpevolezza* (Milano, Giuffrè).

Giunta, Fausto (1997), "Il diritto penale dell'ambiente in Italia: tutela di beni o tutela di funzioni?", *Rivista Italiana di Diritto e Procedura Penale*, pp. 1102 ss.

Grasso, Giovanni (1986)"L'anticipazione della tutela penale: i reati di pericolo e i reati di attentato",", *Rivista Italiana di Diritto e Procedura Penale*, pp. 689 ss.

Insolera, Gaetano, Stortoni, Luigi, "Le vicende della punibilità", *Introduzione al sistema penale*, a cura di Insolera, Gaetano, II Ed., (Torino, Giappichelli), pp. 413 ss.

Lamanuzzi, Marta (2017), "Diritto penale e trattamento dei dati personali. Codice della privacy, novità introdotte dal regolamento UE 2016/679 e nuove responsabilità per gli enti", *Rivista di Scienze Giuridiche*, 1, pp. 221 ss.

Manes Vittorio, Mazzacuva Francesco (2019), "GDPR e nuove disposizioni penali del Codice privacy", *Diritto penale e Processo*, fasc. 2, p. 171 ss.

Manna, Adelmo (1989), *Beni della personalità e limiti della protezione penale*, (CEDAM, Padova).

Manna, Adelmo (1993), "La protezione penale dei dati personali nel diritto italiano", *Rivista trimestrale diritto penale dell'economia*, pp. 179 ss.

Manna, Adelmo (2001), "Il trattamento dei dati personali: le sanzioni penali", in Fiora-vanti, Laura (a cura di), *La tutela penale della persona. Nuove frontiere, difficili equilibri* (Milano, Giuffrè), pp. 339 ss.

Manna, Adelmo (2004), "Codice della privacy: nuove garanzie per i cittadini nel Testo unico in materia di protezione dei dati personali", *Diritto penale e processo*, 1, pp. 17-31.

Manna, Adelmo (2005), "Privacy on line: quali spazi per la tutela penale", *Diritto dell'internet*, pp. 257 ss.

Manna, Adelmo (2010), "I soggetti in posizione di garanzia", *Diritto dell'informazione dell'informatica*, pp. 779-794.

Manna, Adelmo, Di Florio, Mattia (2019), "Riservatezza e diritto alla privacy: in particolare la responsabilità per omissionem dell'internet provider", in Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele (a cura di), *Cybercrime* (Milano, Utet), p. 892 ss.

Mantovani, Ferrando (1968), "Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi", *Arch. giur.*, p. 61 ss.

Mantovani, Ferrando (2017), *Diritto Penale. Parte Generale* (Padova, Cedam).

Mantovani, Ferrando (2016) *Diritto Penale. Parte Speciale*, *Delitti contro la persona*, Vol. I (Padova, Cedam).

Marinucci, Giorgio (1987), "Profili di una riforma del codice penale", *Beni e tecniche della tutela penale. Materiali per la riforma del codice* (Milano, Franco Angeli), pp. 19 ss.

Militello, Vincenzo, Spena, Alessandro (2018), *Mobilità, sicurezza e nuove frontiere tecnologiche* (Torino, Giappichelli).

Mucciarelli, Francesco, "Informatica e tutela penale della riservatezza", in Picotti, Lorenzo (2004), *Il diritto penale dell'informatica* (Padova, Cedam), pp. 173 ss.;

Musco, Enzo (1974), *Bene giuridico e tutela dell'onore* (Milano, Giuffrè).

Musotto, Giovanni (1936), *Le condizioni obiettive di punibilità nella teoria generale del reato* (Palermo, Tumminelli).

Nuvolone, Pietro (1955), *Il diritto penale del fallimento e delle altre procedure concorsuali*, (Milano, Giuffrè).

Padovani, Tullio (1984), "La problematica del bene giuridico e la scelta delle sanzioni", *Dei delitti e delle pene*, pp. 114-131

Padovani, Tullio (1987), "Tutela di beni e tutela di funzioni nella scelta tra delitto, contravvenzione e illecito amministrativo", *Cassazione Penale*, pp. 670 ss.

Pagliaro Antonio (1960), *Il fatto di reato* (Palermo, G. Priulla)

Pagliaro, Antonio (1965), "Bene giuridico e interpretazione della legge penale", *Studi in onore di Francesco Antolisei*, pp. 389 ss.

Pagliaro, Antonio (2003), *Principi di diritto penale. Parte generale* (Milano, Giuffrè).

Pagliaro, Antonio (2003), *Principi di diritto penale. Parte Speciale* (Milano, Giuffrè).

Palamara, Luca (2005), "Note in tema di rilevanza penale del trattamento illecito dei dati personali", *Cassazione Penale*, pp. 1898 ss.

Palazzo, Francesco (1975) "Considerazioni in tema di tutela della riservatezza (a proposito del nuovo art. 615-bis c.p.)", *Rivista Italiana di Diritto e procedura Penale*, p. 126 ss.

Parodi Giusino, Manfredi (1999), "La condotta nei reati a tutela anticipata", *Indice Penale*, pp. 687 ss.

Patrono, Paolo (1986), Voce *Privacy e vita personale (diritto penale)*, *Enc. dir.*, XXXV, pp. 557 ss.

Picotti, Lorenzo (1993), *Il dolo specifico. Un'indagine sugli 'elementi finalistici' delle fattispecie penali* (Milano, Giuffrè).

Picotti, Lorenzo (2012), "I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali", *Giurisprudenza di merito*, 12, pp. 2522

Pisapia, Alice (2018), *La tutela per il trattamento e la protezione dei dati personali* (Torino, Giappichelli)

Pizzetti, Franco (2016), *Privacy e diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento* (Torino, Giappichelli).

Pulitanò, Domenico (1987), "La formulazione delle fattispecie di reato: oggetti e tecniche", *Beni e tecniche della tutela penale. Materiali per la riforma del codice* (Franco Angeli, Milano), pp. 33 ss.

Pulitanò, Domenico (1988), "Una sentenza storica che restaura il principio di colpevolezza", *Rivista Italiana di Diritto e Procedura Penale*, pp. 686 ss.

Ramacci, Fabrizio (2016), *I delitti di omicidio* (Torino, Giappichelli).

Resta, Federica (2019), "I reati in materia di protezione dei dati personali", in Cadoppi Alberto, Canestrari Stefano, Manna Adelmo, Papa Michele, *Cybercrime* (Milano, Utet), p. 1019 ss.

Rodotà, Stefano (2005), *Intervista sulla Privacy* (Bari, Laterza).

Romano, Mario (1992), "Meritevolezza di pena", "bisogno di pena" e "teoria del reato", *Rivista Italiana di Diritto e Procedura Penale*, pp. 39 ss.

Romano, Mario (1995), *Commentario sistematico del codice penale*, II Ed. (Milano, Giuffrè), pp. 319 ss.

Salcuni, Giandomenico (2001)," Natura giuridica e funzioni delle soglie di punibilità nel nuovo diritto penale tributario", *Rivista trimestrale diritto penale dell'economia*, pp. 131-187.

Seminara, Sergio (1998), "Appunti in tema di sanzioni penali nella legge sulla privacy", *Responsabilità Civile e previdenza*, pp. 911 ss.

Sgubbi, Filippo (1998), "Profili penalistici della L. 675/1996", *Rivista trimestrale diritto penale dell'economia*, pp. 75 ss.

Troncone, Pasquale (2011), *Il delitto di trattamento illecito dei dati personali* (Torino, Giappichelli).

Troncone, Pasquale (2014), "Il caso Google (e non solo), il trattamento dei dati personali e i controversi requisiti di rilevanza penale del fatto", *Cassazione Penale*, 6, pp. 2066 ss.

Veneziani, Paolo (2001), "I beni giuridici tutelati dalle norme penali in materia di riservatezza informatica e disciplina dei dati personali", in Fioravanti, Laura (a cura di), *La tutela penale della persona. Nuove frontiere, difficili equilibri* (Milano, Giuffrè), pp. 369 ss.

Vigevani, Giulio Enea (2016), "Diritto all'informazione e privacy nell'ordinamento italiano: regole e eccezioni", *Rivista dell'informazione e dell'informatica*, 3, pp. 473-498.

Warren, Samuel, Brandeis, Louis (1890), "The right to privacy", *Harvard Law Review*, 4, pp. 193-220.

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL

A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

http://dpc-rivista-trimestrale.criminaljusticenetwork.eu