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).

L'utilizzo dello *smartphone* alla guida nei delitti di omicidio e lesioni colpose stradali

El uso del smartphone al momento de conducir en los delitos de asesinato y lesiones culposas

The Usage of Smartphones While Driving and The Traffic-Related Crimes of Manslaughter and Personal Negligence-Based Injuries

Giacomo Maria Evaristi
Dottorando di ricerca presso l'Università di Camerino
giacomo.evaristi@unicam.it

Colpa | Culpa | Negligence

Abstracts

Il crescente fenomeno della distrazione tecnologica del conducente alla guida di veicoli ha reso necessario che, in caso di scontro con esiti lesivi di beni primari, si volgesse l'attenzione allo *smartphone* contestualmente ai rilievi descrittivi. Così alcune Procure della Repubblica hanno emanato direttive finalizzate a contenere abusi degli organi di polizia giudiziaria, senza pregiudicare l'accertamento delle responsabilità penale per i delitti di omicidio e lesioni colpose stradali. In questo quadro si rileva l'utilità del *file* di *log*, documento digitale auto-generato dal dispositivo che annota le operazioni di dialogo tra utente-apparecchio secondo sequenze temporali tracciando cronologicamente l'utilizzo compiutone dal conducente. I *file* di *log*, anche con riferimento alle applicazioni di messaggistica istantanea, hanno un *focus* investigativo limitato al se e quando vi è stato l'uso dello *smartphone* o della singola applicazione, impedendo una generalizzata indagine sulle informazioni salvate nel dispositivo. Ancora discusse risultano invece le modalità procedimentali di acquisizione dei dati informatici, per le quali il diritto vivente pare dimenticare il carattere volatile e alterabile della *digital evidence*.

El creciente fenómeno de la distracción tecnológica del conductor de vehículos ha tenido como consecuencia que, en caso de una colisión con resultados lesivos, la atención se dirija al Smartphone. Algunas fiscalías han elaborado directivas a fin de evitar abusos por parte de la policía, sin prejuzgar la responsabilidad penal del conductor. En este contexto, se evidencia la importancia del archivo de registro, documento digital generado por el propio dispositivo que anota las operaciones de dialogo entre el usuario y el aparato. El archivo de registro tiene una utilidad investigativa limitada a si y cuándo se usó el smartphone y la especifica aplicación, impidiendo por tanto una investigación general sobre las informaciones grabadas en el dispositivo. Todavía se discuten los métodos para adquirir datos informáticos, para los cuales el derecho parece olvidar la naturaleza volátil y alterable de la evidencia digital.

The increasing phenomenon of IT distractions for drivers made inevitable, in the event of accidents involving people, checking the smartphone in addition to other crash measurements. Some Italian Prosecutor Offices issued guidelines in order to avoid any abuse by the police, without prejudice to the assessment of criminal liability for the road/traffic-related offences of manslaughter and personal negligence-based injuries. In the said scenario, the log file can be useful, being a digital document self-generated by a device where all the operations performed with it by the driver are recorded over the time. The log files, even in instant messaging apps, have an investigation focus limited to if and when the smartphone or a single app were used, without an overall view of the information

storage. It is still controversial, in turn, how to acquire such data, especially because the case law seems to forget the volatility and unreliability of digital evidence.

Sommario

1. Premessa.

La circolazione stradale rientra nel gruppo di attività pericolose giuridicamente autorizzate per via del beneficio che la collettività ne trae dallo svolgimento[1].

In tale settore, l'ordinamento fissa uno stretto reticolo di norme a contenuto cautelare, sia generico che specifico[2], con l'obiettivo di eliminare o quantomeno ridurre il rischio di eventi lesivi, in particolare dei beni della vita e dell'integrità fisica dei consociati[3].

Tra le maggiori cause di incidenti stradali si evidenzia la c.d. distrazione tecnologica prodotta dall'utilizzo dello *smartphone* (o *tablet*) durante la marcia[4]: il conducente distoglie la propria attenzione dalla strada per taluni secondi, poiché intento ad operare sul dispositivo elettronico, finendo per perdere il controllo del proprio veicolo, ovvero non avendo la giusta prontezza nell'affrontare le situazioni della circolazione. In particolare, l'utilizzo dell'apparecchio radiotelefonico, in ragione dello sviluppo tecnologico che lo ha interessato negli ultimi anni, attrae l'attenzione per numerose possibilità di utilizzo, che inducono il conducente a spostare lo sguardo dal percorso, creando dei momenti di vuoto di dominio sull'autovettura.

Con riferimento al rilievo penale di tali condotte, si deve premettere che il legislatore nel 2016 ha affrancato le fattispecie di omicidio colposo e lesioni colpose stradali, al fine di costituire una adeguata risposta repressiva nei confronti delle condotte imprudenti alla guida dei veicoli[5]. All'interno di tali nuove fattispecie, speciali per specificazione, il legislatore è intervenuto a graduare il rimprovero attraverso la previsione di circostanze aggravanti c.d. indipendenti per le condotte che manifestano un maggior allarme sociale, contravvenendo le elementari disposizioni cautelari in materia di circolazione stradale[6].

La distrazione tecnologica alla guida costituisce una delle nuove sfide alla prevenzione penale, facendo perno sulla disposizione specifica dell'art. co. 173 co. 2 Codice della Strada, che vieta l'utilizzo di apparecchi radiotelefonici da parte di chi si trova alla guida del veicolo.

Poiché ai fini dello scrutinio in ordine alla integrazione di questa fattispecie colposa si richiede, tra l'altro, la prova della violazione della regola cautelare a contenuto specifico, il ganglio centrale dell'accertamento penale concerne propriamente se vi sia stato l'utilizzo del dispositivo alla guida negli attimi immediatamente precedenti l'evento naturalistico occorso. Si conferma così l'assunto della centralità, nel procedimento penale, della *digital evidence*, la quale non ha rilievo limitato ai soli reati digitali, bensì anche alle fattispecie ove il dispositivo elettronico è strumento, anche solo occasionale, di realizzazione della condotta tipica[7].

Tale esigenza di ricostruzione ed accertamento della dinamica dell'incidente automobilistico, può ricevere fondamentale supporto dai c.d. *file* di *log*. Invero, il sistema operativo o le singole applicazioni dell'apparecchio radiotelefonico annotano, con data ed orario, le attività compiute nell'interfacciarsi con il dispositivo. L'insieme delle suddette informazioni viene raggruppato ed ordinato temporalmente, secondo una scansione temporale precisa, all'interno del

[1] Mantovani (2015), p. 173.

[2] Si è posto in luce che le norme contenenti prescrizioni positive di condotta presentano comunque un contenuto ampio, sicché devono essere definite elastiche.

[3] Siamo dinanzi alle c.d. regole cautelari improprie, giacché il loro scopo è quello di contenere il livello di rischio entro un *range* di accettabilità, senza di bloccare ab origine lo svolgimento di una determinata attività lesiva come prescrivono le c.d. regola cautelari proprie). Su questa distinzione, si esprime P. Veneziani, (2003), p. 20 s.

[4] L'ISTAT svolge annualmente analisi dei dati sui sinistri stradali, indicando il numero di vittime o feriti che sono ascrivibili a tale circostanza. Le informazioni, relative al 2017, sono riportante nel seguente link: https://www.istat.it/it/files/2018/07/Incidenti-stradali_2017.pdf

[5] La ragione della scelta di politica criminale deve essere ricondotta alla trasformazione del contenuto del *dolo eventuale*. Il superamento della teoria dell'accettazione del rischio, rimpiazzata dalla c.d. teoria del bilanciamento con richiamo alla. *formula di Frank*, fatta propria dalla Cass. pen., Sez. Un. 18/09/2014 n. 38343, Espenhahn, ha ricondotto le fattispecie delittuose causate dalla violazione di regole cautelari, dapprima agevolmente riconducibili al dolo, nell'alveo della responsabilità colposa, la cui risposta sanzionatoria non era considerata adeguata al disvalore sociale di tale condotta.

[6] Il riferimento è alle alterazioni psicofisiche per assunzione di sostanze stupefacenti, ovvero per stato di ebrezza ovvero ancora per specifiche condotte che contravvengono le basilari disposizioni che regolano la circolazione stradale, quale la inversione del senso di marcia in prossimità di intersezioni, ovvero per chi raggiunge elevati spread di velocità rispetto ai limiti consentiti.

[7] Luparia, (2007a), p. 131.

c.d. *file* di *log*. Tale documento digitale può essere generato dal dispositivo (*log* di sistema), dalle singole applicazioni (di messaggistica istantanea ad esempio), ovvero anche dal *web* server.

Lasciando fuori dalla presente disamina le informazioni immagazzinate dai gestori di *server* o della rete, la cui acquisizione risulterebbe maggiormente problematica da vari punti di vista, non c'è dubbio che pare enorme la forza epistemica delle notizie archiviate *off-line* nel dispositivo del conducente del veicolo coinvolto nel sinistro: esse potrebbero assumere significativo peso nell'accertamento della responsabilità colposa di chi si trovava alla guida dell'autovettura la cui marcia ha determinato il decesso di una persona o altri gravi danni alla sua integrità psico-fisica. In effetti, i *data* di tali *file* se posti a sistema con altre evidenze processuali[8], quali le testimonianze, le informazioni ricavate da apparecchi elettronici installati sui veicoli (c.d. scatola nera), o, ancora, filmati delle registrazioni di videocamere installate nel luogo pubblico dello scontro, consentirebbero di accertare se l'evento lesivo sia eziologicamente ascrivibile alla violazione della disposizione di cui all'art. 173 co. 2 CdS.

2. Quali diritti e garanzie per lo *smartphone*?

Prima di concentrare l'attenzione sulla specifica valenza probatoria del *file* di *log*, è necessario vagliare il regime giuridico-processualistico dello *smartphone*, con riferimento alle informazioni in esso immagazzinate.

È innegabile che tale dispositivo abbia acquistato, nel corso degli ultimi anni, un peso fondamentale nella vita quotidiana, in quanto rappresenta il mezzo attraverso cui l'individuo estrinseca la propria personalità e alimenta la propria dimensione sociale e relazionale, gestendo costantemente i propri affari in modo ergonomico. Per tale ragione, l'ordinamento protegge, dietro la minaccia della sanzione penale, *id est* ai sensi dell'art. 615-ter c.p., i sistemi elettronici ed informatici da accessi abusivi.

Sorvolando la discussione in ordine alla natura del bene giuridico presidiato dalla norma incriminatrice, che solo apparentemente pare sovrapponibile alla discussione qui condotta, si deve chiarire quale tutela vada riconosciuta all'utilizzatore dello *smartphone*, ed ai dati in esso presenti, dinanzi all'attività investigativa dell'autorità finalizzata ad accertare se ve ne sia stato un utilizzo durante la marcia.

Ai fini di una analitica trattazione delle problematiche sottese a queste nuove entità, non pare peregrino distinguere una duplice dimensione dello *smartphone*, una di natura statica, immagazzinatrice di informazioni o *data*, ed una dinamica, in relazione alla sua idoneità di generare flussi di informazioni e comunicazioni. Se con riferimento al secondo aspetto, le compressioni della libertà e segretezza delle comunicazioni devono muoversi entro il perimetro di tutela delineato dall'art. 15 Cost, nello specifico della riserva di legge, della garanzia giudiziaria e del principio di motivazione, il discorso pare da impostare diversamente in relazione ai dati immagazzinati nel dispositivo, ivi compresi *sms*, le *e-mail* ovvero i messaggi inviati attraverso le applicazioni di dialogo istantaneo (*Whatsapp*, *Messanger* ecc) e memorizzati nel dispositivo ovvero nei *server* cui il dispositivo costituisce la porta di accesso. Tali dati, infatti, non rientrano nella categoria di intercettazioni delle comunicazioni, neppure nella declinazione informatica, e pertanto possono essere considerati come giacenti al di fuori dall'usbergo degli artt. 15 Cost. e 266 e ss. c.p.p.[9].

Deve essere quindi presa in considerazione un'ulteriore dimensione del dispositivo elettronico, quella correlata al suo essere contenitore di informazioni autoprodotte o semplicemente salvate e catalogate e, in relazione a tale dimensione, ci si deve interrogare, da un lato, su quali possano essere i presidi sulla cui base predicare la inviolabilità del dispositivo rispetto ad eventuali invasioni della Pubblica autorità per esigenze investigative; dall'altro, a quali condizioni la Pubblica autorità può superare tali presidi per appropriarsi delle preziose informazioni contenute nei cellulari di nuova generazione.

Tenuto conto del fondamentale rilievo che lo *smartphone* possiede nell'espletamento delle azioni quotidiane, configurando una articolazione spaziale, pur se non fisica, ove si proietta costantemente la sfera più intima della persona, si può affermare che quel luogo, pur se solo virtuale, possa assumere il valore di *domicilio* di cui all'art. 14 Cost. Sposando, dunque, un'in-

[8] Ha sostenuto la ridotta «autonomia dimostrativa» della prova digitale, L. Luparia, (2007b), p. 145.
[9] Cfr. Cass. pen., Sez. V., 21/11/2017, n. 1822.

terpretazione evolutiva, e non storica della disposizione costituzionale testé richiamata, il diritto fondamentale si estenderebbe anche all'involucro materiale, non limitandosi alla garanzia della riservatezza dei dati ivi contenuti[10].

Dando conto, invece, dell'impostazione più diffusa nel diritto vivente, sviluppatasi anche sull'approfondimento teorico della giurisprudenza costituzionale tedesca la quale ha riconosciuto il diritto alla segretezza ed integrità dell'informazione contenuta nel dispositivo informatica, quale declinazione evolutiva del diritto alla dignità personale[11], l'art. 2 Cost. si manifesta come norma generale che, nel tutelare la dignità fondamentale, presidia la c.d. riservatezza informatica la cui resistenza ad invasioni dell'autorità, per finalità investigative, si fonda sul carattere *contra legem*, nonché sproporzionato, dell'attività strumentale al perseguimento delle responsabilità penali. Tale attività di permeazione nello spazio digitale dell'individuo, prima compiuta con interpretazioni estensive dei mezzi di ricerca della prova tipizzati, ha riacquisito una nuova tipicità, specifica per il dominio 'informatico', in ragione dell'adozione della convenzione di Budapest sul *cybercrime* (l. 18 marzo 2008 n. 48).

3. L'incidente stradale: i primi rilievi e l'attenzione allo *smartphone*.

Puntando al cuore del tema oggetto di trattazione, va evidenziato che in caso di scontro tra veicoli cui conseguono esiti letali a beni primari, è pronto l'intervento degli agenti di pubblica sicurezza, al fine di ripristinare i flussi della circolazione, nonché a svolgere i rilievi di polizia giudiziaria, con lo scopo di raccogliere gli elementi utili prodromici all'accertamento delle eventuali responsabilità penali.

Nel cennato frangente, la constatazione che tali incidenti lesivi della integrità fisica, talora anche letali, siano stati causati dall'utilizzo dello *smartphone* alla guida ha imposto una riflessione in ordine alle attività da espletare nell'immediatezza dello scontro, al fine di far compenetrare nelle azioni investigative tanto l'interesse a non disperdere i dati salvati nel dispositivo, utili ai fini dell'accertamento, quanto la riduzione del rischio di arbitrarie apprensioni da parte della Polizia giudiziaria.

In tale direzione, plurali Procure della Repubblica sul territorio nazionale, come ad esempio quelle presso i Tribunali del Friuli Venezia Giulia, ovvero presso i Tribunali di Trento o Modena, hanno emanato direttive che regolano gli accertamenti da compiere nella *scena criminis*, strumentali a verificare se il sinistro sia riconducibile all'uso dello *smartphone* durante la guida.

In particolare, il documento elaborato dalla Procura presso il Tribunale trentino prescrive che solo in presenza di elementi di fatto da cui poter ricavare presumibilmente che l'incidente fosse ascrivibile ad una distrazione c.d. elettronica[12], è possibile procedere ad un visivo esame, *id est* ispezione, sullo *smartphone* o altro dispositivo rinvenuto nell'abitacolo[13].

La cennata direttiva specifica altresì che i rilievi, ai sensi dell'art. 354 co. 2 c.p.p.[14] devono essere espletati dall'ufficiale di polizia giudiziaria, e solo in casi eccezionali dagli agenti, secondo la previsione dell'art. 114 disp. att., previo avvertimento della facoltà di nomina del difensore (356 c.p.p.).

Tale primo accertamento è comunque subordinato al consenso del proprietario e si limita nell'esame del dispositivo (applicazioni in funzione, schermate attive) nonché alle condizioni esterne dell'apparecchio, le cui risultanze sono annotate nel contestuale processo verbale. Il mezzo di ricerca della prova 'tipico', pur se espletato secondo le cennate modalità, espone all'evidente rischio di alterare la genuinità del dato informatico, che presenta elevato tasso di vo-

[10] In questo senso, R. Borruso, (1994), p. 28: secondo cui il dispositivo informatico è organo del singolo individuato, poiché è il contenitore «di tutte le conoscenze, i ricordi, i segreti».
[11] Sul tema affrontato dalla Corte Costituzionale tedesca, si veda il commento di Flor, (2009), p. 695 s.
[12] Si provvede ad una esemplificazione degli stessi: l'apparecchio viene rinvenuto sul tappetino anteriore, ovvero vicino ai piedi del conducente; la presenza del dispositivo acceso o in funzione di vivavoce; lo *smartphone* presenta rotture della scocca.
[13] Si tratterebbe di indagine informatica «non occulta» in quanto espletata sotto la percezione del soggetto destinatario, secondo la classificazione operata da M. Daniele, (2017), p. 267.
[14] È evidente infatti che il Pubblico Ministero non abbia ancora assunto la direzione delle indagini in ragione del peculiare atteggiarsi di tale vicenda rilevante per il diritto penale

latilità[15] ed alterabilità[16]. Inoltre l'eventuale riscontro visivo circa lo stato di accensione ovvero la presenza di applicazioni attive conduce in ogni caso ad una conoscenza marginale, che può presentarsi irrilevante o comunque insufficiente[17]. Si verrebbe a contraddire la regola basilare dell'attività di rilievo investigativo sul dato informatico che necessita di una cautela particolare al fine di evitare le contaminazioni dall'esterno tali pregiudicare il valore della *digital evidence*[18].

Nell'ipotesi di esito negativo dell'esame visivo dello *smartphone* condotto come detto su consenso del titolare, il dispositivo verrà restituito al titolare, con precisa indicazione nel verbale.

Diversamente, ove si ravvisano elementi fattuali che possano far presumere l'utilizzo del telefono, prosegue la direttiva, il dispositivo deve essere sottoposto a sequestro ai sensi dell'art. 354 co. 2 c.p.p., nel rispetto della procedura di custodia (assicurare che il dispositivo non si spenga, nonché escludere l'accesso al sistema da remoto mediante l'attivazione della specifica funzione, c.d. modalità aereo, ovvero mediante la creazione di una schermatura di alluminio o di gabbia di faraday). Si prevede specificamente anche l'invito rivolto al proprietario dell'apparecchio a fornire il PIN, previa comunicazione che pur in caso di diniego si provvederà con l'accesso forzato ai contenuti ivi presenti, anche a costo di danneggiarli[19]; mentre per ciò che concerne le modalità di custodia, ove la misura cautelativa involga una pluralità dispositivi rinvenuti negli abitacoli, essi verranno inseriti in buste differenti.

4. Il sequestro dello *smartphone* e del *file* di *log*.

Come già annunciato, l'attività ispettiva della polizia giudiziaria sul dispositivo elettronico nell'immediatezza dell'incidente non pare la soluzione più efficace in punto di successo investigativo. In effetti, il reperimento di elementi per sostenere l'accusa per omicidio o lesioni colpose stradali potrebbe, in modo più utile, transitare per il vaglio del *file* di *log*. Tale *metadato* digitale racchiude le operazioni compiute dall'utente con l'apparecchio, secondo uno specifico ordine temporale, ed è autoprodotto dal dispositivo che provvede a conservalo. Come di evidente valutazione, il *file di log* del sistema o delle singole applicazioni rappresenta una prova documentale che soggiace all'art. 234 c.p.p. di cui è consentita l'acquisizione poiché rappresenta il fatto «*mediante un qualsiasi altro mezzo*».

In tale senso, l'apparecchio che ha generato l'informazione e che materialmente la ospita si presenta solo come fonte di prova, giacché, come detto, l'elemento di prova ha natura digitale, e corrisponde specificamente al relativo documento digitale.

In questo senso occorre valutare se e in che limiti il dispositivo può essere sottoposto a vincolo di indisponibilità, funzionale all'estrazione di quell'informazione rilevante per l'accertamento della responsabilità penale. Ciò che va precisato è che l'ablazione dello *smartphone* è funzionale al sequestro probatorio del documento digitale ivi contenuto, il c.d. *file* di *log*, la cui estrazione non potendo avvenire nella contestualità dell'azione, dovrà essere condotta in diversa sede. Ne consegue che la misura cautelare ablativa deve essere supportata da elementi di fatto che sorreggano la prospettazione dell'utilizzo dello *smartphone* durante la marcia.

La complessità e le peculiarità dei sistemi informatici dello *smartphone*, con architetture differenti rispetto agli apparecchi fissi, impongono altresì di meditare sulle tecniche di *forensics analysis* per estrarre le informazioni salvate nel dispositivo mobile, anche alla luce dei differenti sistemi operativi installati (*Android*; *iOS*)[20].

La misura cautelare del sequestro del dispositivo è teleologicamente orientata all'estrazione di una copia digitale del *file di log*, Il vincolo di indisponibilità sull'apparecchio fisico viene quindi meno, dopo l'estrazione del documento digitale, espletata in modo tale da assicurare l'originalità del dato nonché la possibilità di svolgere (ripetibili) valutazioni sullo stesso.

[15] Per via della *data persistance* che impone un accertamento comunque nell'immediatezza e non a distanza di tempo, pena la cancellazione o sovrascrittura dei dati

[16] Sulla peculiarità del dato informatico, che presenterebbe i caratteri dell'immaterialità e fragilità intrinseca, si veda Di Bitonto, (2008) p. 504.

[17] Ciò in quanto le applicazioni possono rimanere attive nel dispositivo per lungo tempo, pur senza che le stesse siano in uso.

[18] Così espressamente prevede l'art. 354 co. 2 c.p.p. come modificato per via dell'art. 9 co, 3 l. 48/2008 che ha dato attuazione alla Convenzione di Budapest del Consiglio d'Europa sul Crimine informatico.

[19] Su tale indicazione, si rinvengono ombre della violazione del diritto al silenzio.

[20] I dispositivi mobili sono operano attraverso le c.d. memorie NAND Flash per i quali non sarebbe possibile svolgere una copia *bit* a *bit*.

Ne consegue che il vincolo di indisponibilità sulla *res* fisica non essendo supportato da alcuna altra ragione, dovrà essere travolto. Ciò consente di assicurare la conformità al principio di proporzionalità del vincolo che illumina l'intera disciplina della ingerenza dell'autorità nell'ambito procedimento penale[21].

5. Attività investigativa informatica e tutela del contraddittorio.

La creazione della *bit stream image*, o comunque di un intervento similare atto a fotografare i contenuti del dispositivo mobile, richiede di interrogarsi in ordine alla garanzie procedimentali in tale sede. In effetti, la copia forense può essere generata mediante l'utilizzo di particolari *software* a disposizione degli organi inquirenti, che assicurano l'assoluta identità con i dati originali. Tale attività di copiatura non può comunque essere svolta nell'immediatezza dei rilievi in sede di incidente stradale, poiché è richiesta una particolare strumentazione e competenze settoriali per la sua creazione.

Con riferimento a questo tema, ancora discussa risulta essere la possibilità che la cennata operazione d'indagine, e cioè l'estrazione della copia dei dati contenuti del dispositivo, debba essere espletata alla stregua di un accertamento tecnico irripetibile.

La giurisprudenza ha affermato che tale intervento investigativo non implica alcuna attività valutativa di carattere tecnico-scientifico dell'organo inquirente, né risulta essere compromesso il valore della genuinità dell'informazione in ragione del fatto che il dato potrà essere oggetto di continue valutazioni, senza rischio di alterazione[22].

La ricostruzione sposata dalla giurisprudenza di legittimità è stata sottoposta a critica nella parte in cui, con disinvoltura, non riconosce la singolarità dell'azione investigativa su elementi informatici, per i quali il concetto di irripetibilità dovrebbe specificarsi, in questo settore, nel diverso significato di *volatilità* o *alterabilità* della *digital evidence*[23].

L'attività d'indagine attraverso cui si procede all'estrazione della *bit strem image* dovrebbe essere espletata in modo tale da assicurare la garanzia del diritto di difesa del soggetto sospettato del reato, secondo le modalità dell'accertamento tecnico irripetibile (art. 360 c.p.p.), atteso che le conoscenze tecniche necessarie per tale intervento non sono comuni e comunque, come detto, la caratteristica di alterabilità dei dati impone la necessaria cristallizzazione del dato probatorio, ancor prima della sede normale di formazione della prova, il dibattimento[24].

Seguendo l'indirizzo tracciato dalla giurisprudenza per cui l'estrazione di una copia forense deve essere effettuata unicamente nel rispetto delle *best practices* elaborate dalla *computer forensics*, si ricava che la garanzia dell'integrità della *bit stream image* rispetto al dato originale viene adeguatamente assicurata dalla etichetta generata dalla funzione di *hash*[25]. Particolare cura deve essere poi riservata anche alla conservazione della copia forense, così da scongiurare che sulla stessa intervengano alterazioni *medio tempore*, e comunque prima dell'espletamento delle analisi processuali sulla *digital evidence*[26].

6. L'equilibrio per il *file* di *log*.

Ai fini dell'accertamento della responsabilità dei reati di omicidio e lesioni colpose stradali, l'interesse finalizzato all'accertamento non investe tutti i dati informatici contenuti nel dispositivo, bensì può essere limitato solo a quei *file* che registrano le operazioni di dialogo tra l'utente e la macchina, da cui poter ricavare la specifica scansione temporale di tale uso nel

[21] In punto di sproporzione del vincolo reale, Cass. pen., Sez. VI, 24 febbraio 2015, n. 24617, in *Cass. pen.,* 1, 2016, p. 286.; in generale, si veda Caianello (2014) p. 143 s.; nonché, in chiave più specifica, Nicolicchia, (2018), p. 1 s.

[22] In questo senso, tra le prime pronunce, Cass. pen., Sez. I, 5 marzo 2009, n. 14511, Aversano Stabile, in Cass. pen., 4, 2010, p. 1520 e ss, con nota di Lorenzetto . Cass. pen., Sez. I, 9 marzo 2011, n. 17244, in Cass. pen., 2, 2012, p. 440 con commento critico di Daniele il quale evidenzia come è indimostrato che l'oggetto dell'indagine informatica non venga modificato a seguito dell'estrazione del dato digitale. Sulla stessa linea interpretativa, a seguire, Cass. pen., Sez. V, 16 novembre 2015, n. 11905, Branchi, *CED* 266477.

[23] Marafioti (2011), p. 4509 s., e spec. 4519.

[24] Lorenzetto (2009), p. 154 s.

[25] Si tratta di una particolare funzione crittografica che assicura la rispondenza della copia rispetto al dato digitale originale che si voleva duplicare.

[26] Si consenta il rinvio generale alla monografia di Signorato (2018) ove l'Autrice ha sistematizzato la materia delle indagini informatiche.

tempo antecedente l'incidente. Si tratta del c.d. *log*, meta-dato che automaticamente genera e raccoglie le informazioni relative al funzionamento del sistema, con il peculiare fine di consentire agli sviluppatori un riscontro dei problemi tecnici del sistema operativo o della singola applicazione.

Orbene, per l'accertamento di reati in esame, tale *digital evidence* può rappresentare un equilibrato compromesso tra l'interesse ad un efficace accertamento dell'utilizzo dello *smartphone* alla guida causativo di morte o lesioni personali – cui si correla la funzione di prevenzione generale nei confronti di un fenomeno dalla pervicace diffusione[27] – e le libertà fondamentali, in particolare la riservatezza e la libertà delle comunicazioni; quest'ultima viene in rilievo qualora il guidatore-utente stesse utilizzando programmi per lo scambio di messaggi.

In effetti, maggiore cautela deve essere poi assegnata ai *file* di *log* ovvero ai *file* di cronologia delle applicazioni di messaggistica istantanea, ad esempio *Whatsapp*. Seppur le informazioni di cui sopra costituiscono prova documentale e non intercettazione di flussi comunicativi nella modalità informatica[28], per ciò che concerne la specifica questione, e cioè se lo scontro tra veicoli sia ascrivibile all'utilizzo dello *smartphone* durante la marcia, l'interesse investigativo è limitato al solo dato esterno della conversazione, ulteriormente scremato: non è rilevante infatti conoscere il contenuto del messaggio né il destinatario/mittente, bensì l'attenzione deve concentrarsi solo sull'*an* ed il tempo in cui il guidatore abbia violato la regola cautelare distraendo la propria attenzione dal controllo dell'autovettura, così da ricostruire se vi è stata distrazione tecnologica in grado causare l'evento naturalistico (morte o lesioni gravi o gravissime)[29].

La conoscenza ricavabile dal *file* di *log*, in ogni caso, non è in grado di per sé di raggiungere esiti risolutivi; essa costituisce 'solo' una evidenza da considerare insieme ad altre, sia dichiarative sia documentali. Appare però una soluzione percorribile, giacché senza frustrare la finalità investigativa, assicura una proporzionata, e quindi legittima, invasione del diritto fondamentale al rispetto della vita privata (art. 8 CEDU)[30].

Bibliografia

Borruso Roberto (1994): "La tutela del documento e dei dati" in Borruso Roberto, Buonomo Giovanni, Corasaniti Giuseppe, D'Aietti Gianfranco, *Profili penali dell'informatica*, (Milano, Giuffrè), 1994, p. 28.

Caianello Michele (2014): Il principio di proporzionalità nel procedimento penale, in *Diritto penale contemporaneo – Rivista Trimestrale*, 3-4, p. 143 s.

Daniele, Marcello (2012): "*Il diritto al preavviso della difesa nelle indagini informatiche*", in *Cassazione penale*, 2, p. 441 s.

Daniele, Marcello (2017): "Le indagini informatiche contro il terrorismo", in Wein Roberto, Fornasari Gabriele (a cura di), *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, (Trento, Editoriale Scientifica), p. 267.

Daniele, Marcello (2018): "La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge", in *Processo penale e giustizia*, 5, p. 831 s.

Di Bitonto, Maria Lucia (2008): "L'accertamento investigativo delle indagini sui reati informatici", in *Diritto dell'internet*, 5, p. 504.

[27] La possibilità di ricostruire con certezza se lo scontro tra veicoli sia ascrivibile alla violazione dell'art. 173 co. 2 CdS porta con sé un'indubbia forza deterrente avverso tali distrazioni per la generalità dei consociati.
[28] Si rinvia a nt. 9.
[29] Si coglie in effetti la preoccupazione esternata in materia di indagini informatiche, pur se con peculiare riferimento alle forme di captazione dei dati *on-line* da M. Daniele, (2018), p. 831 s.
[30] Tra gli ultimi arresti in materia di limiti all'ingerenza arbitraria dell'autorità nella vita privata, con riferimento all'attività di perquisizione, Corte e.d.u. del 27/09/2018, Brazzi contro Italia, ric. n. 57278/11, § 41.

Flor Roberto (2009): "Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung", in *Rivista trimestrale di diritto penale dell'economia*, 3, p. 695.

Lorenzetto, Elisa (2010): *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in Cassazione penale, 4, p.

Lorenzetto Elisa (2009): "Le attività urgenti di investigazione informatica e telematica", in Luparia Luca (a cura di), Sistema penale e criminalità informatica (Milano, Giuffrè), p. 154 e ss.

Luparia, Luca (2007a): "Processo penale e scienza applicata", in Luparia Luca, Ziccardi Giovanni, *Investigazione penale e tecnologia informatica*, (Milano, Giuffrè), p. 131.

Luparia, Luca (2007b): "La ricerca della prova digitale", in Luparia Luca, Ziccardi Giovanni, *Investigazione penale e tecnologia informatica*, (Milano, Giuffrè), p. 145.

Mantovani, Ferrando (2015): "*Diritto Penale, Parte generale*", (Padova, CEDAM), p. 173.

Marafioti, Luca (2011): "*Digital evidence* e processo penale", in *Cassazione penale*, 12, 2011, p. 4509 s.

Nicolicchia Fabio (2018): "Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova", in *www.penalecontemporaneo.it*, 8/01/2018, p. 1 s.

Signorato, Silvia (2018): *Le indagini digitali. Profili strutturati di una metamorfosi investigativa* (Torino, Giappichelli).

Veneziani Paolo (2003): "*Regole cautelari "proprie" ed "improprie"*", (Padova, Cedam), p. 20 s.