

C J N

# Diritto Penale Contemporaneo

R I V I S T A T R I M E S T R A L E

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

#### EDITOR-IN-CHIEF

Gian Luigi Gatta

#### EDITORIAL BOARD

*Italy:* Antonio Gullo, Guglielmo Leo, Luca Luparia, Francesco Mucciarelli, Francesco Viganò  
*Spain:* Jaime Alonso-Cuevillas, Sergi Cardenal Montraveta, David Carpio Briz, Joan Queralt

Jiménez

*Chile:* Jaime Couso Salas, Mauricio Duce Julio, Héctor Hernández Basualto, Fernando Londoño Martínez

#### MANAGING EDITOR

Carlo Bray

#### EDITORIAL STAFF

Alberto Aimi, Enrico Andolfatto, Enrico Basile, Javier Escobar Veas, Stefano Finocchiaro, Elisabetta Pietrocarlo, Tommaso Trinchera, Stefano Zirulia

#### EDITORIAL ADVISORY BOARD

Rafael Alcacer Guirao, Alberto Alessandri, Giuseppe Amarelli, Ennio Amodio, Coral Arangüena Fanego, Lorena Bachmaier Winter, Roberto Bartoli, Fabio Basile, Hervé Belluta, Alessandro Bernardi, Carolina Bolea Bardón, David Brunelli, Silvia Buzzelli, Alberto Cadoppi, Pedro Caeiro, Michele Caianiello, Lucio Camaldo, Stefano Canestrari, Francesco Caprioli, Claudia Cárdenas Aravena, Raúl Carnevali, Marta Cartabia, Elena Maria Catalano, Mauro Catenacci, Massimo Ceresa Gastaldo, Mario Chiavario, Mirentxu Corcoy Bidasolo, Cristiano Cupelli, Norberto Javier De La Mata Barranco, Angela Della Bella, Cristina de Maglie, Gian Paolo Demuro, Miguel Díaz y García Conlledo, Ombretta Di Giovine, Emilio Dolcini, Jacobo Dopico Gomez Áller, Patricia Faraldo Cabana, Silvia Fernández Bautista, Javier Gustavo Fernández Terruelo, Marcelo Ferrante, Giovanni Fiandaca, Gabriele Fornasari, Novella Galantini, Percy García Caveró, Loredana Garlati, Mitja Gialuz, Glauco Giostra, Víctor Gómez Martín, José Luis Guzmán Dalbora, Ciro Grandi, Giovanni Grasso, Giulio Illuminati, Roberto E. Kostoris, Máximo Langer, Juan Antonio Lascurain Sánchez, Maria Carmen López Peregrín, Sergio Lorusso, Ezequiel Malarino, Francisco Maldonado Fuentes, Stefano Manacorda, Juan Pablo Mañalich Raffo, Vittorio Manes, Grazia Mannozi, Teresa Manso Porto, Luca Marafioti, Joseph Margulies, Enrico Marzaduri, Luca Maserà, Jean Pierre Matus Acuña, Anna Maria Maugeri, Oliviero Mazza, Iván Meini, Alessandro Melchionda, Chantal Meloni, Melissa Miedico, Vincenzo Militello, Santiago Mir Puig, Fernando Miró Linares, Vincenzo Mongillo, Renzo Orlandi, Francesco Palazzo, Carlenrico Paliero, Michele Papa, Raphaële Parizot, Claudia Pecorella, Marco Pelissero, Lorenzo Picotti, Paolo Pisa, Oreste Pollicino, Domenico Pulitanò, Tommaso Rafaraci, Paolo Renon, Mario Romano, María Ángeles Rueda Martín, Carlo Ruga Riva, Stefano Ruggeri, Francesca Ruggieri, Marco Scoletta, Sergio Seminara, Paola Severino, Nicola Selvaggi, Rosaria Sicurella, Jesús María Silva Sánchez, Carlo Sotis, Giulio Ubertis, Inma Valeije Álvarez, Antonio Vallini, Paolo Veneziani, Costantino Visconti, Javier Willenmann von Bernath, Francesco Zacchè

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.

Il lettore può leggere, condividere, riprodurre, distribuire, stampare, comunicare al pubblico, esporre in pubblico, cercare e segnalare tramite collegamento ipertestuale ogni lavoro pubblicato su "Diritto penale contemporaneo – Rivista trimestrale", con qualsiasi mezzo e formato, per qualsiasi scopo lecito e non commerciale, nei limiti consentiti dalla licenza Creative Commons - Attribuzione - Non commerciale 3.0 Italia (CC BY-NC 3.0 IT), in particolare conservando l'indicazione della fonte, del logo e del formato grafico originale, nonché dell'autore del contributo.

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](mailto: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 con 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 protección 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](mailto: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.

Visitors to the site may share, reproduce, distribute, print, communicate to the public, search and cite using a hyperlink every article published in the journal, in any medium and format, for any legal non-commercial purposes, under the terms of the Creative Commons License - Attribution – Non-commercial 3.0 Italy (CC BY-NC 3.0 IT). The source, logo, original graphic format and authorship must be preserved.

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](mailto: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](#)).

IL DIRITTO PENALE  
NEL CYBERSPAZIO

*EL DERECHO PENAL  
EN EL CIBERESPACIO*

*CRIMINAL LAW  
IN CYBERSPACE*

<b>Neutralization Theory: Criminological Cues for Improved Deterrence of Hacker Crimes</b>	1
<i>“Teoría de la neutralización”: tra prevención e repressione del cybercrime</i>	
<i>“Teoría de la neutralización”: Entre prevención y represión del cibercrimen.</i>	
Marcello Sestieri	

<b>«Send nudes» Il trattamento penalistico del sexting in considerazione dei diritti fondamentali del minore d'età</b>	9
<i>El tratamiento penal del sexting en consideración a los derechos fundamentales de los menores de edad</i>	
<i>The Criminalisation of Sexting Involving Underage Victims</i>	
Domenico Rosani	

<b>Gli effetti dell'automazione sui modelli di responsabilità: il caso delle piattaforme online</b>	33
<i>Los efectos de la automatización en los modelos de responsabilidad: el caso de las plataformas online</i>	
<i>The Effects of Automation on Imputation Models: the Case of Online Platforms</i>	
Beatrice Panattoni	

DIRITTO PENALE E  
LIBERTÀ DI ESPRESSIONE  
IN INTERNET

*EL DERECHO PENAL Y LA  
LIBERTAD DE EXPRESIÓN EN  
INTERNET*

*CRIMINAL LAW AND  
FREEDOM OF EXPRESSION  
ON THE INTERNET*

<b>Istanze di criminalizzazione delle fake news al confine tra tutela penale della verità e repressione del dissenso</b>	60
<i>La criminalización de las fake news entre al confín entre tutela penal de la verdad y represión del disenso</i>	
<i>Criminalisation of Fake News Between the Protection of Truth and the Suppression of Dissent</i>	
Anna Costantini	

<b>Il volto dei reati di opinione nel contrasto al terrorismo internazionale al tempo di Internet</b>	81
<i>El rostro de los delitos de opinión en la lucha contra el terrorismo internacional en la época de Internet</i>	
<i>The Face of Word Crimes in the Fight Against International Terrorism at the Time of the Internet</i>	
Paolo Cirillo	

<p><i>FINANCIAL</i> <i>CYBERCRIME</i></p> <p><i>CIBERCRIMEN</i> <i>FINANCIERO</i></p> <p><i>FINANCIAL</i> <i>CYBERCRIME</i></p>	<p><b>Crowdfunding @ ICOs: esigenze di prevenzione del rischio di commissione di reati nell'era della digital economy</b> 101</p> <p><i>Crowdfunding @ ICOs: exigencias de prevención del riesgo de comisión de delitos en la era de la economía digital</i></p> <p><i>Crowdfunding @ ICOs: Commission Risk Prevention Needs of Crimes in the Era of the Digital Economy</i></p> <p>Antonietta di Lernia</p>
	<p><b>La tutela penale del segreto commerciale in Italia.</b> 112</p> <p><b>Fra esigenze di adeguamento e possibilità di razionalizzazione</b></p> <p><i>La tutela penal del secreto comercial en Italia.</i></p> <p><i>Entre exigencias de adecuación y posibilidades de racionalización</i></p> <p><i>The Protection of Trade Secret under Italian Criminal Law.</i></p> <p><i>Between Needs for Adequacy and Options for Rationalization</i></p> <p>Riccardo Ercole Omodei</p>
	<p><b>L'abuso di mercato nell'era delle nuove tecnologie.</b> 129</p> <p><b>Trading algoritmico e principio di personalità dell'illecito penale</b></p> <p><i>Abuso del mercado en la era de las nuevas tecnologías.</i></p> <p><i>Trading algorítmico y principio de responsabilidad penal personal</i></p> <p><i>Market Abuse in the Age of New Technologies.</i></p> <p><i>Algorithmic Trading and Principle of Individual Criminal Responsibility</i></p> <p>Marta Palmisano</p>
	<p><b>Gli strumenti di prevenzione nazionali ed europei in materia di valute virtuali e riciclaggio</b> 148</p> <p><i>Los instrumentos de prevención nacional y europeos en materia de monedas virtuales y lavado de activos</i></p> <p><i>Domestic and European Preventative Instruments Concerning Virtual Currencies and Money Laundering</i></p> <p>Cristina Ingraio</p>
	<p><b>Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione</b> 159</p> <p><i>Las monedas virtuales y los ontológicos riesgos de lavado de activos: técnicas de represión.</i></p> <p><i>Virtual currencies and the endemic risk of money laundering: repression techniques</i></p> <p>Fabiana Pomes</p>

<p>LA TUTELA PENALE DELLA PRIVACY NEL CYBERSPAZIO</p> <p><i>LA TUTELA PENAL DE LA PRIVACIDAD EN EL CIBERESPACIO</i></p> <p><i>CRIMINAL LAW AND THE PROTECTION OF PRIVACY IN CYBERSPACE</i></p>	<p><b>I limiti della tutela penale del trattamento illecito dei dati personali nel mondo digitale</b></p> <p><i>Los límites de la tutela penal del tratamiento ilícito de datos personales en el mundo digital</i></p> <p><i>Limits to Criminalization of Unlawful Data Processing in the Digital World</i></p> <p>Salvatore Orlando</p>	<p>178</p>
	<p><b>Il compendio sanzionatorio della nuova disciplina privacy sotto la lente del <i>ne bis in idem</i> sovranazionale e della Costituzione</b></p> <p><i>El compendio sancionatorio de la nueva regulación de la privacidad bajo la lente del ne bis in idem internacional y de la Constitución italiana</i></p> <p><i>The Sanctioning System for Privacy-Related Infringements from the Supranational Ne Bis In Idem and the Italian Constitution Perspectives</i></p> <p>Ludovica Deaglio</p>	<p>201</p>
	<p><i>Eternal Sunshine of the Spotless Crime.</i></p> <p><b>Informazione e oblio nell'epoca dei processi su internet</b></p> <p><i>Eternal Sunshine of the Spotless Crime.</i></p> <p><i>Información y olvido en la época de los procesos de internet</i></p> <p><i>Eternal Sunshine of the Spotless Crime.</i></p> <p><i>The Right to Information and the Right to be Forgotten in Times of Trials by Media</i></p> <p>Edoardo Mazzanti</p>	<p>212</p>
	<p><b>La moltiplicazione dei garanti nel settore della tutela dei dati personali: riflessi penalistici del GDPR</b></p> <p><i>La multiplicación de las garantías en el sector de la tutela de los datos personales: Reflexiones penalísticas del GDPR</i></p> <p><i>The Multiplication of Responsibilities in the Personal Data Protection Area: Criminal Law Implications of the GDPR</i></p> <p>Gaia Fiorinelli</p>	<p>239</p>
	<p><i>Corporate liability e compliance in the cyber privacy crime:</i></p> <p><b>il nuovo “modello organizzativo privacy”</b></p> <p><i>Responsabilidad corporativa y compliance en el delito de privacidad cibernética: El nuevo “modelo organizativo de privacidad”</i></p> <p><i>Corporate Liability and Compliance in the Cyber Privacy Crime: the New “Privacy Organizational Model”</i></p> <p>Valentina Aragona</p>	<p>251</p>

<p>SICUREZZA INFORMATICA, COMPLIANCE E PREVENZIONE DEL RISCHIO DI REATO</p> <p><i>SEGURIDAD INFORMÁTICA, COMPLIANCE Y PREVENCIÓN DEL RIESGO DE DELITOS</i></p> <p><i>IT SECURITY, COMPLIANCE AND CRIME PREVENTION</i></p>	<p><b>I discorsi d'odio nell'era digitale: quale ruolo per l'internet service provider?</b></p> <p><i>Los discursos de odio en la era digital: ¿Cuál es el rol del proveedor de servicios de internet?</i></p> <p><i>Hateful Speech in the Digital Era: Which Role for the ISP?</i></p> <p>Valérie Nardi</p> <hr/> <p><b>Big Data Analytics e compliance anticorruzione</b></p> <p><b>Profili problematici delle attuali prassi applicative e scenari futuri</b></p> <p><i>Análisis de Big Data y compliance anticorrupción</i></p> <p><i>Cuestiones críticas de la práctica actual y escenarios futuros</i></p> <p><i>Big Data Analytics and Anti-corruption Compliance</i></p> <p><i>Critical Issues of Current Practice and Future Scenarios</i></p> <p>Emanuele Birritteri</p> <hr/> <p><b>La partita del diritto penale nell'epoca dei "drone-crimes"</b></p> <p><i>El partido del derecho penal en la era de los "delitos de dron"</i></p> <p><i>The Criminal Law Match in the Era Of "Drone-Crimes"</i></p> <p>Carla Cucco</p> <hr/> <p><b>Profili penalistici delle self-driving cars</b></p> <p><i>Cuestiones de derecho penal en relación a los vehículos de conducción autónoma</i></p> <p><i>Self-driving Cars and Criminal Law</i></p> <p>Alberto Cappellini</p> <hr/> <p><b>Gli algoritmi predittivi per la commisurazione della pena.</b></p> <p><b>A proposito dell'esperienza statunitense nel c.d. evidence-based sentencing</b></p> <p><i>Los algoritmos predictivos para la determinación de la pena. A propósito de la experiencia estadounidense del "evidence-based sentencing"</i></p> <p><i>Predictive Algorithms for Sentencing. The US Experience of the So-Called Evidence-Based Sentencing</i></p> <p>Luca D'Agostino</p> <hr/> <p><b>Banche dati, attività informativa e predittività. La garanzia di un diritto penale del fatto.</b></p> <p><i>Bases de datos, actividades de información y predictibilidad. La garantía de un derecho penal del hecho</i></p> <p><i>Databases, Information Activities and Prediction. The Safeguard of Fact-related Criminal Law</i></p> <p>Pietro Sorbello</p>	<p>268</p> <p>289</p> <p>304</p> <p>325</p> <p>354</p> <p>374</p>
---	--	---

NUOVE TECNOLOGIE E PROCESSO PENALE  <i>NUEVAS TECNOLOGÍAS Y          PROCESO PENAL</i>  <i>NEW TECHNOLOGIES AND          CRIMINAL PROCEDURE</i>	<b>Algoritmi predittivi: alcune premesse metodologiche</b> 391 <i>Algoritmos predictivos: algunas premisas metodológicas</i> <i>The 'multi-faceted' brain of predictive algorithms.</i> Barbara Occhiuzzi
	<b>Algoritmi predittivi e discrezionalità del giudice:          una nuova sfida per la giustizia penale</b> 401 <i>Algoritmos predictivos y discrecionalidad del juez:          un nuevo desafío para la justicia penal</i> <i>Predictive Algorithms and Judicial Discretion:          a New Challenge for Criminal Justice</i> Lucia Maldonato
	<b>Le nuove indagini tecnologiche e la tutela dei diritti fondamentali.          L'esperienza del captatore informatico</b> 417 <i>Las nuevas tecnologías de investigación y la tutela de los derechos fundamentales. La          experiencia del software espía</i> <i>New IT-based Investigations and Protection of Fundamental Rights.</i> <i>The Case of Spy-software</i> Gaia Caneschi
	<b>Il controllo occulto e continuativo come categoria probatoria:          premesse teoriche di una sistematizzazione</b> 430 <i>El control oculto y continuado como categoría probatoria: premisas teóricas de una          sistematización</i> <i>The Hidden and Continous Control as Evidentiary Notion: Theoretical Premises for          a Systematic Analysis</i> Fabio Nicolichia
	<b>L'accesso transfrontaliero all'electronic evidence, tra esigenze          di effettività e tutela dei diritti</b> 439 <i>El acceso transfronterizo a evidencia electrónica, entre exigencias          de efectividad y tutela de derechos</i> <i>Transnational Access to Electronic Evidence Between Effectiveness          and the Need to Protect Rights</i> Veronica Tondi

---

<b>L'utilizzo dello <i>smartphone</i> alla guida nei delitti di omicidio e lesioni colpose stradali: l'accertamento processuale della colpa attraverso i c.d. <i>file di log</i>.</b>	456
<i>El uso del smartphone al momento de conducir en los delitos de asesinato y lesiones culposas: la verificación procesal de la culpa a través del archivo de registro</i>	
<i>The Usage of Smartphones While Driving and The Road/Traffic-Related Crimes of Manslaughter and Personal Negligence-Based Injuries: the Assessment of Negligence in Court Through the So-Called Log Files.</i>	
Giacomo Maria Evaristi	

---

<b>Spunti per una riflessione sul rapporto fra biometria e processo penale</b>	465
<i>Ideas para reflexionar sobre la relación entre biometría y proceso penal</i>	
<i>Ideas for a Reflection on the Relationship Between Biometrics and Criminal Trial</i>	
Ernestina Sacchetto	

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*

# La moltiplicazione dei garanti nel settore della tutela dei dati personali: riflessi penalistici del GDPR

*La multiplicación de las garantías en el sector de la tutela de los datos personales: Reflexiones penalísticas del GDPR*

*The Multiplication of Responsibilities in the Personal Data Protection Area: Criminal Law Implications of the GDPR*

GAIA FIORINELLI

Allieva perfezionanda in Diritto Penale presso la Scuola Superiore Sant'Anna di Pisa  
gaia.fiorinelli@santannapisa.it

PRIVACY

PRIVACY

PRIVACY

## ABSTRACTS

L'individuazione delle posizioni di garanzia nel settore della tutela dei dati personali costituisce un tema quasi inesplorato, sia da parte degli studiosi della materia, sia da parte della giurisprudenza, di merito e di legittimità. Tale tema, tuttavia, merita un rinnovato interesse a seguito dell'entrata in vigore del Regolamento Europeo per la Protezione dei Dati Personali e del relativo decreto di adeguamento (d.lgs.101/2018): è la stessa architettura di tali complessi normativi, infatti, a polarizzare l'attenzione sulla gestione del rischio e sulla *accountability* dei soggetti individuati quali garanti dell'integrità e della sicurezza dei dati e dei sistemi informatici. Il presente contributo mira, dunque, alla ricostruzione delle posizioni di garanzia nel settore della tutela dei dati e al conseguente inquadramento delle relazioni intersoggettive tra i garanti.

La individualización de las posiciones de garantía en el sector de la tutela de los datos personales constituye un tema casi inexplorado, tanto por la doctrina como por la jurisprudencia. No obstante, la entrada en vigencia del Reglamento Europeo de Protección de Datos Personales y del correspondiente decreto de adecuación (Decreto Legislativo 101/2018) justifican una mayor atención a esta materia. El presente artículo tiene por objeto analizar la reconstrucción de las posiciones de garantía en el sector de la tutela de los datos y el consecuente encuadramiento de las relaciones intersubjetivas entre las garantías.

The attribution of responsibility as a 'guarantor' in the area of personal data protection is a relatively unknown issue, both for the scholars and the case-law. The said topic, however, deserves to be (re-)investigated after the entry into force of the EU Regulation on Personal Data Protection, as implemented in Italy by the Legislative Decree no. 101/2018. The legal architecture itself focuses on risk management and accountability of those labelled as 'guarantors' of data integrity and security of networks. This paper aims to reconstruct the notion of 'guarantor' in the area of data protection as well as assessing the relationships among 'guarantors'.

**SOMMARIO**

1. Il GDPR: impostazione preventiva e scopi di tutela. – 2. La moltiplicazione dei garanti nel settore della sicurezza dei dati. – 3. Le relazioni intersoggettive tra i garanti: affidamento e trasferimento di funzioni di tutela. – 4. Conclusioni.

**1.****Il GDPR: impostazione preventiva e scopi di tutela.**

Per quanto il *Regolamento Generale sulla Protezione dei Dati*<sup>1</sup> nulla disponga direttamente in materia penale<sup>2</sup>, l'impostazione complessiva e gli scopi di tutela del *Regolamento* offrono, tuttavia, spunti di notevole interesse anche in una prospettiva penalistica.

Anzitutto, infatti, con l'entrata in vigore del *Regolamento* 679/2016 si è ulteriormente consolidato un approccio di stampo preventivo alla protezione dei dati personali<sup>3</sup>: il titolare del trattamento – sul quale ricade “la responsabilità generale per qualsiasi trattamento di dati personali” (*Considerando* n. 74) – è, infatti, tenuto ad adottare misure idonee a soddisfare i principi della “protezione dei dati fin dalla progettazione” e della “protezione dei dati per impostazione predefinita” (*Considerando* n. 78), così predisponendo già *prima* del trattamento adeguate forme di tutela *mediante la tecnologia*<sup>4</sup>; inoltre, al titolare è altresì richiesto di adottare misure di carattere tecnico e organizzativo adeguate per garantire, *durante* il trattamento, il rispetto delle disposizioni del *GDPR* (*Considerando* n. 78), per la tutela dei diritti e delle libertà delle persone fisiche<sup>5</sup>.

Ulteriore riconferma di tale impostazione preventiva si ritrova, inoltre, nel *Considerando* n. 84, ove si prevede che il titolare del trattamento sia chiamato a svolgere una “valutazione d'impatto sulla protezione dei dati”, qualora il trattamento stesso possa presentare un rischio elevato; mediante tale valutazione si dovrebbero determinare, in particolare, l'origine, la natura, la particolarità e la gravità del rischio, in modo da adottare misure specifiche ed opportune, per assicurare il rispetto del *Regolamento*.

Indicativo dell'importanza della struttura organizzativa è, altresì, l'art. 32 co. 4 del *Regolamento*, in forza del quale il titolare del trattamento è reso responsabile dei trattamenti effettuati da parte dei dipendenti inseriti nell'organigramma aziendale: si prevede, infatti, che il titolare debba far sì che «chiunque agisca sotto la [sua] autorità e abbia accesso ai dati personali» non possa, comunque, trattare tali dati se non sia stato destinatario di specifiche istruzioni in tal senso da parte del titolare.

Orbene, il generale principio di *accountability*<sup>6</sup>, l'accento posto sulle misure *tecniche ed organizzative*, unitamente alla previsione di strumenti di *risk-assessment* – al fine di *prevenire* il rischio di violazioni – consentono di annoverare anche il *GDPR* tra quegli interventi normativi che portano a un progressivo consolidamento del paradigma di «prevenzione mediante organizzazione», con ciò intendendosi la correlazione che si viene a creare tra “gestione del rischio” e organizzazione dei fattori produttivi<sup>7</sup> o, in altri termini, la «estensione totalizzante dell'autoresponsabilità in ogni fase della vita dell'impresa»<sup>8</sup>.

<sup>1</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

<sup>2</sup> Di diretto interesse penalistico è, infatti, soltanto il *Considerando* 149, ove si riconosce agli Stati membri la facoltà di prevedere sanzioni penali per le violazioni del *Regolamento* o delle norme nazionali adottate in attuazione del *Regolamento* stesso. Si prevede, inoltre, che tra le misure penali potrebbe altresì ricomprendersi la sottrazione dei profitti che siano stati illecitamente ottenuti, mediante violazioni di disposizioni del *Regolamento*. Da ultimo, si prescrive che l'adozione di sanzioni penali non possa, tuttavia, porsi in contrasto con il principio del *ne bis in idem*, per come interpretato dalla Corte di Giustizia dell'Unione Europea, rispetto alle sanzioni amministrative, già previste dal *Regolamento*. Sul d. lgs. 101/2018, adottato per adeguare la legislazione nazionale alle disposizioni del *GDPR*, v. MANES, MAZZACUVA (2019), pp. 171 ss.; D'AGOSTINO (2019); LABIANCA (2019), pp. 1004 ss.; RESTA (2019), pp. 1019 ss.; PROVOLO (2019), pp. 242 ss.

<sup>3</sup> Cfr. D'AGOSTINO (2019), p. 53: invero, il sistema di protezione dei dati personali delineato dal *GDPR* sembra «ruotare attorno al concetto di rischio».

<sup>4</sup> Cfr. VOIGT e VON DEM BUSSCHE (2017), p. 38. È l'art. 25 del *Regolamento*, poi, a precisare che tali misure, finalizzate a “integrare nel trattamento le necessarie garanzie” possano consistere, ad esempio, nella pseudonimizzazione, nella minimizzazione, nonché in impostazioni predefinite tali da assicurare che siano trattati soltanto i dati personali necessari per ogni specifica finalità del trattamento.

<sup>5</sup> Cfr. VOIGT e VON DEM BUSSCHE (2017), p. 38.

<sup>6</sup> Cfr. D'AGOSTINO (2019), p. 17, che sottolinea come il principio dell'*accountability*, o dell'autoresponsabilizzazione, attribuisca peculiare importanza alla autodisciplina e alla *compliance*, facendo ricadere sul titolare e sul responsabile l'obbligo di individuare le misure necessarie per assicurare il rispetto di tutte le rilevanti disposizioni di legge.

<sup>7</sup> Così GARGANI (2017), p. 509.

<sup>8</sup> Cfr. D'AGOSTINO (2019), p. 17 e p. 52, ove l'Autore rileva come proprio le imprese, gli enti collettivi (o finanche i grandi attori economici) siano i soggetti sui quali la disciplina del *Regolamento* sembra essere stata plasmata, considerando l'importanza che assumono, nell'impostazione

Si tratta, del resto, di un paradigma di tutela che era stato già messo in luce non soltanto da parte della Corte di Cassazione Civile, a Sezioni Unite, che aveva riconosciuto come dal trattamento di dati personali derivino «obblighi organizzativi, gestionali e di sicurezza la cui corretta individuazione, oltre che dalle specifiche indicazioni normative, discende dalla considerazione della *funzione (di garanzia) della disciplina nel suo complesso*»<sup>9</sup>, ma anche da parte della Corte di Cassazione Penale, che aveva ricostruito la posizione del titolare del trattamento, ponendo in luce l'esistenza, in capo a quest'ultimo, di «un potere decisionale in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati», che si estrinseca anche mediante la designazione dei soggetti responsabili e la gestione dei rischi specifici connessi al trattamento<sup>10</sup>.

Inoltre, come si è anticipato, anche l'ampiezza degli orizzonti di tutela del *Regolamento* si rivela di estremo interesse. Infatti, oltre a tale relevantissima evoluzione strutturale, il *Regolamento Generale sulla Protezione dei Dati* sembra ampliare le prospettive di tutela, dal momento che, come sottolineato dal *Considerando* n. 75, mediante le misure di *protezione* dei dati personali si intende far fronte ai rischi suscettibili di cagionare, addirittura, «un danno fisico, materiale o immateriale», ai diritti e alle libertà delle persone fisiche coinvolte<sup>11</sup>.

È il *Considerando* n. 85, inoltre, a precisare che le «violazioni» dei dati personali possano rilevare anche in quanto suscettibili di tradursi direttamente in più gravi condotte lesive, tra cui discriminazione, furto, usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica<sup>12</sup>.

Con il *GDPR* si è, infatti, portata a compimento la progressiva transizione da una tutela della riservatezza intesa in senso minimalistico quale diritto alla *non divulgazione* delle informazioni di carattere personale, a una tutela effettiva, intesa in un'accezione funzionale, che si traduce nel diritto alla *protezione* e al *corretto trattamento* dei dati personali, o in altre parole, nel diritto alla *corretta gestione* delle informazioni<sup>13</sup>.

Ne deriva, dunque, un quadro composito, nel quale i soggetti individuati dal *Regolamento* quali garanti della protezione e della sicurezza dei dati – e nei cui confronti ricade, dunque, una responsabilità generale – vengono ad essere responsabilizzati in una pluralità di direzioni, a fronte, per l'appunto, della crescente natura plurioffensiva degli illeciti in materia di dati personali<sup>14</sup>.

Non sembra azzardato, dunque, ipotizzare che possano configurarsi forme di responsabilità penale, a carico dei garanti della tutela dei dati, ulteriori rispetto alle sole fattispecie contenute nel *Codice privacy*: come si è detto, infatti, le violazioni delle disposizioni del *Regolamento* potrebbero chiamare in causa fattispecie ulteriori, connesse alla tutela dell'identità digitale, alla sicurezza dei sistemi informatici e finanche alla protezione della reputazione e del patrimonio<sup>15</sup>. Ad esempio, le c.d. *data breaches*, prese in considerazione dal *Regolamento* con riguardo agli obblighi di segnalazione e definite dall'art. 4 n. 12 come quelle violazioni di sicurezza che comportano «accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati», potrebbero con tutta evidenza acquisire rilevanza penale, ai sensi degli

---

generale del *GDPR*, gli obblighi di natura gestionale e organizzativa.

<sup>9</sup> Cfr. RICCI (2018), p. 2648, ove si richiama Cassazione civile., sez. un., 27 dicembre 2017, n. 30984, su *dejure.it*, ove, per l'appunto, espressamente si riconosce che «il legislatore richiede “modalità organizzative” ovvero *condotte positivamente rivolte* a tutelare la riservatezza dei dati».

<sup>10</sup> Cfr. Cassazione penale, sez. III, 17 dicembre 2013, n. 5107, su *dejure.it*; v. anche MANNA, DI FLORIO (2019), pp. 902 ss.

<sup>11</sup> Cfr. MANNA, DI FLORIO (2019), p. 936, ove si rileva, per l'appunto, come una delle novità più importanti del *Regolamento* consista proprio nella «qualificazione del diritto alla protezione dei dati personali come un diritto fondamentale delle persone fisiche (art. 1, par. 2)».

<sup>12</sup> Cfr. MANES, MAZZACUVA (2019), p. 72, ove si sottolinea, per l'appunto, come la fattispecie di cui all'art. 167 del *Codice privacy* («Trattamento illecito di dati personali») risulti incentrata prevalentemente sulla tutela di beni giuridici individuali; in tal senso, la centralità del «nocumento» di cui alla medesima disposizione è chiaro indice della «logica di tutela personalistica» che si è perseguita con la riforma.

<sup>13</sup> In questi termini, cfr. in particolare D'AGOSTINO (2019), p. 8 e p. 10: «il comune cittadino che fruisce dei servizi della società dell'informazione è posto nell'impossibilità di non svelarsi nell'agire quotidiano. Egli rilascia continuamente dati personali che scompongono la sua identità sociale in un catalogo di informazioni, perdendo lentamente il controllo di sé. Per questo la privacy, comunemente intesa nell'accezione minimale di *right to be let alone*, deve – come si è detto – «mutare il suo contenuto da diritto alla riservatezza a diritto all'autodeterminazione informativa». In tal senso cfr. anche TORRE (2004), p. 41.

<sup>14</sup> Come rilevato da MANES, MAZZACUVA (2019), pp. 172 ss., infatti, l'attuale struttura della risposta (anche penale) agli illeciti in tema di dati personali affianca alla tutela di beni giuridici individuali anche una prospettiva di stampo più pubblicistico, che, sulla base di recenti casi di «utilizzo illecito di ingenti masse di dati personali» ha inteso fronteggiare anche «le ipotesi caratterizzate da maggiore diffusività lesiva».

<sup>15</sup> A tal proposito, per un catalogo delle fattispecie contenute nella parte speciale del codice penale che possano ricondursi all'ambito della tutela dei dati, cfr. NAUWELAERTS (2018), pp. 84 ss.

artt. 615-ter c.p., 635-bis c.p. o 640-ter c.p.<sup>16</sup>.

Anche in considerazione di tale progressivo ampliamento degli orizzonti di tutela pare opportuno, dunque, riflettere sulle implicazioni che tale «passaggio da una impostazione negativa e reattiva ad una positiva e proattiva della protezione dei dati personali»<sup>17</sup> può avere per il diritto penale.

## 2.

### La moltiplicazione dei garanti nel settore della protezione dei dati.

A fronte di tale generale responsabilizzazione del titolare del trattamento – che si traduce, come si è visto, nell’obbligo di adottare una pluralità di misure «il cui comune denominatore è la protezione preventiva del dato»<sup>18</sup> – il *Regolamento* si segnala, altresì, per una moltiplicazione dei garanti nel settore della tutela dei dati personali<sup>19</sup>.

Invero, il GDPR prevede sin dalle *Definizioni* (art. 4) il coinvolgimento di una pluralità di soggetti nell’adempimento degli obblighi in esso previsti: accanto al «titolare del trattamento» (n. 7), ovvero sia «la persona [...] che determina le finalità e i mezzi del trattamento di dati personali», è prevista la figura del «responsabile del trattamento» (n. 8), vale a dire «la persona [...] che tratta dati personali per conto del titolare del trattamento».

Infine, si aggiunge a queste figure anche il *responsabile della protezione dei dati personali* (o DPO), designato «in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati» e, quindi, della capacità di assolvere gli specifici compiti che, ai sensi del GDPR, gli devono essere affidati.

Il *Regolamento*, dunque, individua una serie di soggetti quali destinatari *iure proprio* di diversi compiti e ne istituzionalizza la cooperazione per l’assolvimento degli obblighi ivi previsti, mettendo allo stesso tempo in luce, al *Considerando* n. 79, la necessità di pervenire a una chiara ripartizione delle responsabilità tra i medesimi.

Ebbene, tale dettagliata articolazione dei ruoli e delle sfere di competenza dei soggetti coinvolti nel trattamento dei dati è di notevole interesse in una prospettiva penalistica. In particolare, l’indagine non può che essere svolta in primo luogo precisando e ricostruendo gli obblighi e i poteri impeditivi che ricadono su tali soggetti, e ciò tenendo conto che, nelle diverse proiezioni del «diritto penale del rischio», «l’analisi dei ruoli e delle responsabilità viene tematizzata entro la categoria giuridica della posizione di garanzia»<sup>20</sup>: strumento concettuale al quale è allora necessario far riferimento nell’analizzare le norme del GDPR. Come si è detto, infatti, a conferma dell’opportunità della prospettiva così tratteggiata, la latitudine degli obblighi previsti in capo a titolare, responsabile e DPO, comporta la necessità di verificarne le rispettive responsabilità penali non soltanto rispetto agli illeciti di cui agli artt. 167 e ss. del Codice Privacy, in forma commissiva, ma anche, in forma omissiva, rispetto a violazioni o persino a reati informatici commessi da parte di dipendenti o soggetti terzi<sup>21</sup>.

Muovendo allora dal titolare del trattamento, egli è essenzialmente il soggetto obbligato ad adottare, in forza degli artt. 24 e 32 del *Regolamento*, adeguate misure tecniche ed organizzative, finalizzate a ridurre i rischi per la sicurezza (dei dati e, dunque) delle persone coinvolte<sup>22</sup>. In tal senso, dunque, al medesimo è indubbiamente ascrivibile un obbligo di garanzia *iure proprio*, rispetto alla tutela e alla sicurezza dei dati; obbligo che gli deriva direttamente dall’essere – ai sensi delle definizioni di cui all’art. 4 – colui che *determina le finalità e i mezzi*

<sup>16</sup> Cfr. in tal senso anche LUBERTO (2019), p. 948.

<sup>17</sup> Cfr. RICCI (2018) p. 2648.

<sup>18</sup> Cfr. RICCI (2018), p. 2648.

<sup>19</sup> Sul tema (sia pur con riguardo al diverso ambito dell’articolazione delle responsabilità penali in relazione all’abrogato reato di cui all’art. 169 del Codice Privacy), cfr. anche PICOTTI (2013), p. 68.

<sup>20</sup> Cassazione penale, sez. un., 24 aprile 2014, n.38343, su *dejure.it*.

<sup>21</sup> A tale ultimo proposito, v. MANNA (2010), pp. 779 ss., anche in relazione alla diversa questione della configurabilità della fattispecie di cui all’art. 167 *Cod. privacy* in forma omissiva.

<sup>22</sup> Cfr. l’art. 24 GDPR: 1. *Tenuto conto della natura, dell’ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.* Cfr. anche l’art. 32 GDPR: 1. *Tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.*

*del trattamento di dati personali.* In quanto fulcro del potere decisionale, il titolare del trattamento è, dunque, garante *originario*, rispetto alla liceità del trattamento e alla sicurezza dei dati; inoltre, egli è destinatario in via diretta dell'obbligo di predisporre trattamenti conformi alla disciplina del *GDPR*, di adottare adeguate misure di sicurezza, nonché di effettuare la c.d. *Valutazione d'impatto sulla protezione dei dati* (di cui all'art. 35). D'altra parte, la giurisprudenza penale era giunta ad analoghe conclusioni già prima dell'entrata in vigore del *Regolamento*, avendo rilevato come la pregnanza dei poteri decisionali che ricadono in capo al *titolare* del trattamento – in ordine alle finalità e alle modalità del trattamento, nonché, più in generale, in ordine alle misure funzionali alla “gestione dei rischi” – consentisse di ritenerlo destinatario di specifici obblighi di tutela<sup>23</sup>. Del resto, il contenuto di tali obblighi comprende non soltanto la conformità del trattamento alle disposizioni del *Regolamento*, ma anche la “protezione dei dati”, tenuto conto dei rischi per le persone fisiche coinvolte nel trattamento: proprio in tale obbligo di garanzia, così, configurato, si coglie, dunque, quello “speciale vincolo di tutela” tra il soggetto garante e il titolare del bene, incapace di proteggerlo autonomamente<sup>24</sup>, che consente di ipotizzare l'effettiva sussistenza di un obbligo di carattere *impeditivo*, nella forma dell'obbligo “di controllo”, dovendo il titolare del trattamento adottare misure idonee a proteggere (i dati di) un novero indeterminato di soggetti<sup>25</sup> da rischi specifici, connessi allo svolgimento dell'attività.

Così determinati la fonte e lo specifico contenuto dell'obbligo in parola, occorre, dunque, valutare la sussistenza, quanto meno in astratto, di idonei poteri di carattere impeditivo, necessari perché sia configurabile una complessiva posizione di garanzia in capo al titolare del trattamento; ebbene, come si è anticipato, già la Corte di Cassazione aveva attribuito specifico rilievo alla circostanza che il *titolare* sia proprio colui che – in via esclusiva – determina le finalità e le modalità del trattamento, disponendo, dunque, di un'indiscussa signoria sulla fonte di rischio. Tali considerazioni consentono, perciò, di ritenere che il titolare del trattamento rivesta la funzione di “garante”, rispetto alla tutela di tutti i dati personali che siano stati affidati alla sua protezione.

Indubbiamente più complessa è, invece, la focalizzazione del ruolo e delle responsabilità del *responsabile del trattamento*, identificabile in colui che, per l'appunto, *tratta dati personali per conto del titolare del trattamento*.

A tal proposito, per individuare gli obblighi e i poteri del *responsabile*, occorre anzitutto richiamare l'art. 28 *GDPR*, ove si stabilisce che il titolare del trattamento debba ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del *Regolamento* e garantisca la tutela dei diritti dell'interessato, così coinvolgendo direttamente anche il *responsabile* negli obblighi di adempimento alla normativa. Inoltre, la lett. f) co. 3 dell'art. 28 precisa che il responsabile assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 e, infine, l'art. 32 estende al responsabile – al pari del titolare – l'obbligo di mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio.

Dal complesso di tali disposizioni sembra di potersi concludere che anche il responsabile del trattamento sia – nell'articolazione del *GDPR* – destinatario di una serie di obblighi *iure proprio*, sia pur ben più specifici rispetto a quelli previsti in capo al *titolare*. Sulla base di quanto detto, dunque, si può ritenere che, nei limiti dei propri obblighi e, soprattutto, dei propri (limitati) poteri, anche il *responsabile del trattamento* sia titolare di una funzione di garanzia, quanto alla liceità del trattamento e alla sicurezza dei dati. A tal proposito, è utile rammentare come nella giurisprudenza di legittimità il *responsabile* del trattamento sia stato configurato alla stregua di un “preposto”, il quale, dunque, nel limitato ambito cui sia stato adibito, riveste una funzione analoga a quella del *titolare* del trattamento e deve, dunque, essere considerato, in virtù di tale rapporto di preposizione, destinatario diretto di specifici obblighi di tutela<sup>26</sup>. È bene

<sup>23</sup> Cfr. Cassazione penale, sez. III, 17 dicembre 2013, n. 5107, su *dejure.it*.

<sup>24</sup> Cfr. Cassazione penale, sez. IV, 29 marzo 2019, n. 17491, su *dejure.it*. Sul tema specifico cfr. anche D'AGOSTINO (2019), pp. 9-10: nella società dell'informazione, «la generalità dei consociati [rinuncia] tacitamente alla propria riservatezza e [rilascia] le proprie informazioni personali per accedere ai servizi offerti»; «il comune cittadino che fruisce dei servizi della società dell'informazione è posto nell'impossibilità di non svelarsi nell'agire quotidiano. Egli rilascia continuamente dati personali che scompongono la sua identità sociale in un catalogo di informazioni, perdendo lentamente il controllo di sé». Dopo che l'interessato ha “perso” il controllo sui propri dati ricade, pertanto, sul *titolare* del trattamento l'obbligo di assicurarne la protezione e la corretta gestione.

<sup>25</sup> Cfr. ALESSANDRI e SEMINARA (2018), p. 59.

<sup>26</sup> Cfr. Cassazione penale, sez. III, 17 dicembre 2013, n. 5107, su *dejure.it*.

precisare, tuttavia, che l'obbligo di garanzia sussistente in capo al soggetto designato *responsabile* del trattamento dovrà avere un ambito ben circoscritto, non potendosi estendere all'intera gestione aziendale, ma limitandosi, nel contesto del trattamento svolto per conto del titolare, agli obblighi che il *Regolamento* configura direttamente in capo al *responsabile*, alle istruzioni impartite da parte del titolare, nonché, soprattutto, agli effettivi poteri di intervento<sup>27</sup>.

Ancora più complessa è, infine, la figura, introdotta *ex novo* con il *Regolamento*, del *responsabile della protezione dei dati*, o *data protection officer (DPO)*, cui è dedicata l'intera Sezione IV del Capo IV (relativo ai *Soggetti*).

L'art. 37 prevede, infatti, che il titolare e il responsabile del trattamento in taluni casi debbano<sup>28</sup> – e, comunque, possano<sup>29</sup> – nominare, all'interno della compagine aziendale, un *responsabile della protezione dei dati personali*. Tale soggetto deve essere, per l'appunto, designato in funzione delle sue qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere gli specifici compiti, di cui si dirà, previsti dall'art. 39 del *Regolamento*; per espressa indicazione, il *DPO* potrà essere un *dipendente* del titolare del trattamento, ovvero potrà essere legato a quest'ultimo da un contratto di servizi. L'art. 38 attribuisce, poi, al *DPO* connotati peculiari, prevedendo che il *titolare* e il *responsabile* debbano fornirgli le risorse necessarie per assolvere ai propri compiti, nonché che debbano garantire che allo stesso non sia impartita alcuna istruzione; il *Regolamento* configura così, con riguardo al *DPO*, una posizione denotata da autonomia e indipendenza, nell'assolvimento della propria funzione.

Quanto agli obblighi e ai poteri del *DPO*, l'art. 39 del *Regolamento* vi fa rientrare sia funzioni di natura essenzialmente consultiva e informativa – tra le quali il compito di informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento (lett. a) e di fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati, oltre a sorvegliarne lo svolgimento (lett. c) – sia funzioni di portata ben più vasta, tra le quali spicca, in particolare, il compito di *sorvegliare l'osservanza del Regolamento*, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo (lett. b).

Orbene, com'è evidente, le funzioni che rientrano nel primo ambito potrebbero anche portare a escludere un diretto coinvolgimento del *DPO* nelle responsabilità che ricadono sul *titolare* del trattamento; come si è osservato, la figura del *DPO* sarebbe, con riguardo a questo profilo, per certi versi assimilabile a quella del *Responsabile del Servizio di Prevenzione e Protezione*, il quale, come inizialmente riconosciuto dalla giurisprudenza di legittimità, non sarebbe titolare di una autonoma posizione di garanzia<sup>30</sup>, in virtù dello svolgimento di una funzione di solo supporto informativo. La questione è, tuttavia, ben più complessa, già con riguardo a questo primo profilo, ove si consideri che la Suprema Corte ha, sul punto, progressivamente mutato orientamento, arrivando a ritenere che anche un soggetto che, all'interno della struttura aziendale, svolga un ruolo non gestionale ma di consulenza, abbia purtuttavia l'obbligo giuridico di adempiere diligentemente l'incarico affidatogli e, dunque, di collaborare con i vertici dell'impresa individuando i rischi connessi all'attività e fornendo le opportune indicazioni tecniche per risolverli, con la conseguenza che, in relazione a tale suo compito, potrà essere

<sup>27</sup> A tal proposito può essere utile ricordare quanto previsto dall'art. 82 *GDPR*: *Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.*

<sup>28</sup> Recita, infatti, l'art. 37 *GDPR*: 1. *Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualevolta: a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.*

<sup>29</sup> In virtù dell'art. 37 par. 4 *GDPR*.

<sup>30</sup> In tal senso, v. Cassazione penale, sez. IV, 23 novembre 2012, n. 49821, su *dejure.it*, ove si esclude che il responsabile del servizio di prevenzione e protezione (art. 32 e 33 d.lgs. n. 81 del 2008) sia, in quanto tale, titolare di una posizione di garanzia penalmente rilevante ex art. 40 co. 2 c.p.; ma v. anche Cassazione penale, sez. IV, 10 maggio 2017, n. 27516, su *dejure.it*, ove si è riconosciuta l'esistenza di una posizione di garanzia, sussistente in capo al responsabile del servizio di prevenzione e protezione, ma limitata alla diligente valutazione dei rischi, in modo completo e idoneo, in ciò compendiandosi i suoi obblighi e poteri impeditivi, rispetto all'evento da prevenire. V. anche MASSARO (2013), p. 357 ss., e in part. 362.

chiamato a rispondere, quale garante, degli eventi che si verifichino per effetto della violazione dei suoi doveri<sup>31</sup>.

Le maggiori difficoltà nel definire il ruolo rivestito dalla figura del *DPO* derivano, tuttavia, dalla citata lett. b) dell'art. 39, ove si annovera tra i compiti del *DPO* anche l'obbligo, di portata generale, di sorvegliare l'osservanza del *Regolamento* e delle altre disposizioni rilevanti in tema di protezione dei dati<sup>32</sup>. È necessario comprendere, infatti, se tale obbligo, ove letto in combinazione con i poteri riconosciuti al *DPO* dall'art. 38 del *Regolamento*, costituisca pur sempre obbligo di mera sorveglianza, o venga a configurarsi come obbligo di *garanzia*<sup>33</sup>.

Affatto peculiari sono, infatti, le posizioni di coloro che siano destinatari di un generale obbligo, per così dire, di “vigilare sull'osservanza della legge”, com'è il caso, ad esempio, dei membri del collegio sindacale ai sensi dell'art. 2403 c.c., oppure dei membri dell'Organismo di Vigilanza costituito ai sensi del d. lgs. 231/2001<sup>34</sup>; a tal proposito, infatti, nonostante le indicazioni di segno contrario provenienti dalla dottrina, la Corte di Cassazione ha a più riprese affermato che un dovere consistente nel “controllo di legalità”, qual è quello che ricade, ad esempio, sui membri del collegio sindacale, comporti, ove violato, un coinvolgimento in eventuali reati commessi da parte dei soggetti vigilati, a titolo di omesso impedimento del reato altrui<sup>35</sup>. Né pare che la questione possa essere agevolmente risolta mediante uno scrutinio dei poteri di tipo fattuale e giuridico di cui dispone il *DPO*, che si risolvono essenzialmente in poteri cognitivi e di segnalazione. A tal proposito, infatti, nonostante si sia da più parti rilevata l'esigenza di escludere l'applicazione del meccanismo imputativo di cui all'art. 40 co. 2 c.p. in tutte le ipotesi in cui la legge imponga meri obblighi di sorveglianza<sup>36</sup>, accompagnati da poteri di intervento c.d. “deboli”<sup>37</sup>, è pur vero che, secondo l'impostazione giurisprudenziale dominante<sup>38</sup>, un potere-dovere di segnalazione e di informazione – qual è quello che grava sul *DPO* – costituisce una sorta di potere di intervento “mediato”, funzionale a sollecitare azioni impeditive altrui<sup>39</sup>. Si tratta, com'è evidente, di una questione di amplissimo respiro, che si iscrive nel tema della responsabilità dei soggetti controllori per l'omesso impedimento del reato da parte dei soggetti controllati<sup>40</sup>.

Ciò che si vuole rilevare è, tuttavia, come tale disciplina renda estremamente complesso definire la posizione di garanzia riconducibile al *DPO*. Se, infatti, con riguardo a taluni aspetti potrebbe escludersi che lo stesso sia titolare di una autonoma posizione di garanzia, radicando tale conclusione nei connotati di *professionalità* e nelle funzioni di *consulenza* attribuite a tale soggetto<sup>41</sup>, tuttavia l'autonomia e l'indipendenza che il *GDPR* attribuisce al *DPO*, nonché l'obbligo – *iure proprio* – di tenere conto dei rischi del trattamento<sup>42</sup> e, soprattutto, la previsione di un generale dovere di sorveglianza sull'applicazione del *Regolamento* da parte dei soggetti

<sup>31</sup> In questi termini, Cassazione penale, sez. un., 24 aprile 2014, n. 38343, su *dejure.it*.

<sup>32</sup> Sul punto cfr. WORKING PARTY ARTICLE 29 (2017), p. 17: nell'obbligo di sorvegliare la *compliance* rientrano i compiti relativi alla raccolta di informazioni, al fine di identificare i processi rilevanti e, dunque, di analizzarne la conformità con il *Regolamento*; inoltre, è richiesto al *DPO* di informare, consigliare e fornire proposte di miglioramento al *titolare* e al *responsabile* del trattamento.

<sup>33</sup> A tal proposito è necessario rinviare a LEONCINI (1999), p. 7, che sottolinea la differenza sussistente tra obblighi di *garanzia*, la cui violazione può dar luogo a responsabilità *ex art. 40 co. 2 c.p.*, e obblighi di *attivarsi* e di *sorveglianza*, la cui inosservanza non può mai dare luogo a responsabilità in forma omissiva. In tal senso, in quanto obbligo di controllare l'altrui operato, dovrebbe trattarsi in questo caso di un semplice obbligo di sorveglianza (capace di configurare, dunque, in capo al *DPO* un obbligo di segnalazione e informazione, ma non un obbligo di intervento). In senso analogo cfr. WORKING PARTY ARTICLE 29 (2017), p. 4 e p. 24: il *DPO* non è personalmente responsabile per la *non-compliance* con i requisiti di *data protection* posti dal *Regolamento*.

<sup>34</sup> Cfr. sul punto BISORI (1997); GIUNTA (2006); CENTONZE (2009); CONSULICH (2015).

<sup>35</sup> Cfr. da ultimo Cassazione penale, sez. V, 18 febbraio 2019, n. 12186, su *dejure.it*, nonché CENTONZE (2009), pp. 227 ss.

<sup>36</sup> Cfr. AMBROSETTI, MEZZETTI, RONCO (2012), p. 109.

<sup>37</sup> Cfr. GIUNTA (2006), p. 608.

<sup>38</sup> In giurisprudenza cfr. da ultimo Cassazione penale, sez. IV, 01 febbraio 2018, n. 9167, su *dejure.it*, nonché Cassazione penale, sez. IV, 12 gennaio 2016, n. 20050, su *dejure.it*, ove si statuisce l'equivalenza, ai fini della configurabilità di una posizione di garanzia, tra “poteri atti a impedire la lesione del bene garantito” e la disponibilità di “mezzi idonei a sollecitare gli interventi necessari a evitare che l'evento dannoso sia cagionato”.

<sup>39</sup> Sulla configurazione di poteri impeditivi di carattere mediato, cfr. in generale GARGANI (2017), p. 523; CONSULICH (2015), p. 444, ove si rileva come sia proprio «il concetto di *potere impeditivo mediato* che potrebbe consentire di predicare l'esistenza di una responsabilità omissiva per tutti coloro che sono parte necessaria, seppure non sufficiente, di una procedura impeditiva». Osserva GIUNTA (2006), p. 608, come, invece, possano ritenersi effettivamente impeditivi soltanto quei poteri cui corrispondano «doveri di conformazione, in quanto il loro esercizio produce effetti giuridici vincolanti sull'attività del soggetto controllato, e più in generale i poteri di blocco dell'attività del controllato». Anche DE FRANCESCO (2012), p. 3929, rileva come «l'allentamento della verifica dell'autonomia e concreta capacità impeditiva della condotta doverosa» sia evidente soprattutto laddove si configurino «meri obblighi di sorveglianza» rispetto all'altrui operato.

<sup>40</sup> Cfr. ancora GIUNTA (2006); CENTONZE (2009); CONSULICH (2015).

<sup>41</sup> Sulle *Garantenstellungen* di esperti e consulenti, v. GARGANI (2017), p. 521; BASILE (2018).

<sup>42</sup> Cfr. l'art. 39 par. 2, ove si prevede che 2. *Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.*

coinvolti contribuiscono a configurare una figura di carattere “ibrido”, che non consente di risolvere in senso certamente negativo la questione circa la possibile sussistenza di una posizione di garanzia rilevante ai fini della presente indagine<sup>43</sup>.

Ad ogni modo, pare che anche nelle maglie del *Regolamento* sia possibile cogliere quei due distinti paradigmi che si sono progressivamente affermati nel campo delle *Garantensstellungen* individuali<sup>44</sup>: da un lato, con riguardo alla posizione del *titolare* (e, volendo, del *responsabile*), si è, infatti, costituito un «modello di garanzia incentrato sulla sicurezza mediante prevenzione del rischio lecito»; dall'altro, con riferimento alla posizione del *DPO*, si è, invece, prefigurata una posizione per certi versi riconducibile al modello della «prevenzione del rischio illecito»<sup>45</sup>, trattandosi di un soggetto tenuto non già alla tutela *diretta* dei beni coinvolti, quanto, come detto, alla più generale sorveglianza del rispetto di tutte le disposizioni rilevanti in materia.

### 3. Le relazioni intersoggettive tra i garanti della sicurezza: affidamento e trasferimento di funzioni di tutela.

L'analisi dei ruoli e delle responsabilità dei diversi soggetti normativamente previsti non può, certo, arrestarsi alla mera individuazione delle singole posizioni di garanzia: la sussistenza di vincoli di tutela che, in quanto reticolari, sono altresì interdipendenti, richiede, infatti, di confrontarsi con il tema delle relazioni intersoggettive tra i garanti<sup>46</sup> della tutela dei dati, al fine di comprendere, in particolare, la funzione e l'efficacia, rispetto al *titolare del trattamento*, della nomina del *responsabile del trattamento* e del *responsabile della protezione dei dati*.

A tal proposito, nel vigore della originaria disciplina in materia di protezione dei dati personali di cui alla l. 675 del 1996, si riteneva che il «potere-dovere», rimesso al titolare del trattamento, di decidere e, dunque, indirizzare i trattamenti, non fosse derogabile né, tantomeno, delegabile<sup>47</sup>, cosicché non potessero nemmeno ipotizzarsi forme di trasferimento di funzioni dotate di efficacia liberatoria o quantomeno modificativa dell'originaria posizione di garanzia.

È necessario, tuttavia, verificare se tali conclusioni possano dirsi ancora attuali, dal momento che il *Regolamento* disciplina nel dettaglio le relazioni tra il *titolare* e i suoi “ausiliari”, determinando non soltanto i requisiti che devono caratterizzare ciascun soggetto, ma anche le formalità relative agli atti di nomina, nonché l'efficacia di tali scelte organizzative sull'articolazione delle relative responsabilità.

Muovendo dalle relazioni tra il *titolare* e il *responsabile* del trattamento, quest'ultimo può, come si è anticipato, essere considerato una sorta di “preposto” il quale, in virtù delle norme del *Regolamento* e delle istruzioni impartite dal *titolare*, è destinatario *iure proprio* di obblighi di adeguamento e di impedimento, ma non è dotato di un'autonomia tale da poter in alcun modo esonerare da responsabilità il *titolare* del trattamento in caso di violazioni<sup>48</sup>.

A riconferma di ciò è possibile richiamare la stessa nomenclatura utilizzata dal *GDPR*: se, infatti, la traduzione italiana crea ambiguità, è utile osservare come nel testo originale il *titolare* sia definito *controller*, mentre il *responsabile* sia, invece, un mero *processor*, cui può essere affidato, dunque, un complesso di funzioni di carattere meramente tecnico-esecutivo.

A fronte di ciò è, tuttavia, interessante osservare quanto previsto dall'art. 28 par. 10 del *Regolamento*, ove si prevede che laddove un responsabile del trattamento violi il *Regolamento*, determinando autonomamente le finalità e i mezzi del trattamento, egli sarà considerato un titolare del trattamento in questione. Proprio questa disposizione, infatti, può costituire, in un certo senso, un indice della impossibilità per il *titolare* del trattamento di delegare ad altri le principali funzioni decisionali che gli sono affidate dal *Regolamento*, essendo precluso al *responsabile* qualsiasi intervento nella determinazione generale delle *finalità* e dei *mezzi* del trattamento. Di tale disposizione può, al contempo, darsi una diversa lettura: tale norma, infat-

<sup>43</sup> Ritiene CALZOLAIO (2017), p. 620, che il vero ruolo che il DPO assume è quello di importare, nell'organizzazione del Titolare del trattamento, l'esperienza maturata ed aggiornata in merito alle migliori pratiche attuative ed alle politiche *della privacy by design e by default*.

<sup>44</sup> Cfr. GARGANI (2017), p. 515: si tratta di due distinti paradigmi, accomunati dal medesimo referente teleologico-funzionale, rappresentato dal rischio.

<sup>45</sup> Cfr. ancora GARGANI (2017), p. 515.

<sup>46</sup> Cfr. GARGANI (2017), pp. 514-516 e DE FRANCESCO (2012), pp. 3927 ss.

<sup>47</sup> Cfr. BLAIOTTA (1999), p. 1643.

<sup>48</sup> Cfr. ancora BLAIOTTA (1999), p. 1643, che qualifica come meramente “operativi” i compiti affidati al responsabile del trattamento da parte del titolare.

ti, può essere considerata una sorta di clausola di equiparazione tra soggetti di fatto e soggetti di diritto, cosicché, nel caso in cui le competenze attribuite o le funzioni svolte dal soggetto che sia formalmente *responsabile* del trattamento arrivino fino alla determinazione *autonoma* delle finalità o dei mezzi del trattamento<sup>49</sup>, lo stesso vedrà ricadere su di sé gli obblighi previsti in capo al precedente *titolare del trattamento*, potendosi così ipotizzare un trasferimento – o, meglio, un ampliamento<sup>50</sup> – della corrispondente posizione di garanzia.

Quanto, poi, al diverso tema delle relazioni intersoggettive tra titolare-responsabile del trattamento e *DPO*, è necessaria anche in questo caso qualche ulteriore precisazione.

Come si è anticipato, infatti, in forza dell'art. 38 del *Regolamento* il *DPO* si trova a rivestire una posizione connotata da autonomia e indipendenza nell'assolvimento dei propri compiti, che si traducono in una funzione informativo-consultiva e in una funzione di sorveglianza; inoltre, l'art. 37 – ove si specifica il requisito dell'idoneità professionale del *DPO* – e le prime indicazioni operative in materia<sup>51</sup> portano a ritenere che il *DPO*, in forza della “conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati” possa anche essere attivamente coinvolto nell'adempimento degli obblighi di *compliance*.

Tale molteplicità di funzioni richiede, dunque, di interrogarsi sulle relazioni funzionali che si vengono a creare tra il *DPO* e i garanti “originari”, nella predisposizione delle misure tecniche e organizzative necessarie per la protezione dei dati, dovendosi verificare quali siano gli effetti – ai fini dell'articolazione delle responsabilità – dell'eventuale scelta di demandare al *DPO* decisioni di carattere tecnico od operativo.

Ebbene, a tal proposito, è possibile rammentare, in una prospettiva pratico-applicativa, la già richiamata giurisprudenza della Corte di Cassazione relativa alla figura del *Responsabile del Servizio di Protezione e Prevenzione*, ove si è confermato, a più riprese, che il ruolo dallo stesso svolto non possa essere in alcun modo assimilabile a quello di un “delegato”, trattandosi di una figura normativamente individuata e, dunque, destinataria di *investitura* e non di *delega di funzioni*<sup>52</sup>. Considerazioni di egual segno potrebbero, allora, svolgersi anche con riferimento alla figura del *DPO*, soprattutto nelle ipotesi in cui la sua nomina sia prevista obbligatoriamente dal *GDPR*. È necessario osservare, tuttavia, come l'art. 39, nel prevedere che il *DPO* sia incaricato “almeno” dei compiti che vi sono elencati, non escluda la possibilità di un più ampio coinvolgimento dello stesso *DPO* nell'adempimento degli obblighi di *compliance*, proprio in virtù della richiamata conoscenza specialistica e della funzione di supporto che lo stesso è chiamato a svolgere rispetto al vertice dell'impresa. In tali ipotesi, infatti, ove si considerino l'autonomia decisionale (e finanche di spesa) di cui è dotato il *DPO*, si potrebbe allora ipotizzare che sul *titolare* del trattamento rimanga soltanto un più generale obbligo di *vigilanza*, trasferendosi sul *DPO* l'autonomia decisionale di carattere *tecnico*, rispetto all'individuazione delle *best practices* per l'adempimento degli obblighi previsti dal *GDPR*.

È, ad ogni modo, indubbio che il tema della relazione tra *titolare* e *DPO* si collochi nella ben più ampia questione della “scissione tra potere organizzativo-decisionale e sapere tecnico-scientifico”<sup>53</sup>, una questione che, purtuttavia, è essenzialmente ignorata nella prassi applicativa, com'è reso evidente dalla perdurante tendenza ad accentrare sul vertice dell'impresa (e sul destinatario diretto dei precetti penali) le rispettive responsabilità<sup>54</sup>.

Anche dalla presente analisi emerge, infatti, tale tendenza all'accentramento dei poteri – e delle responsabilità – in capo al *titolare* del trattamento, atteso che, come si è visto, non sembra che atti di investitura o di delega possano con certezza limitarne la complessiva posizione di garanzia.

Ebbene, in tale scenario è allora interessante osservare come nel *Regolamento* sia stato introdotto, all'art. 26, l'istituto della *contitolarietà*, quale strumento funzionale a dare evidenza

<sup>49</sup> Cfr. a tal proposito GARGANI (2017), p. 518, ove si specifica la questione dei “garanti di fatto”, con riguardo a tutte le ipotesi di «scissione tra titolarità formale della qualifica soggettiva e il reale e concreto esercizio della funzione corrispondente».

<sup>50</sup> Cfr. ancora GARGANI (2017), pp. 518-519, ove si rileva come le clausole di equiparazione tra soggetti di diritto e soggetti di fatto e le norme estensive della qualifica comportino la «proliferazione di nuove e ulteriori posizioni di garanzia».

<sup>51</sup> Cfr. ad es. WORKING PARTY ARTICLE 29 (2017), p. 13.

<sup>52</sup> D'ALESSANDRO (2016), p. 242, che sottolinea l'importanza di distinguere l'attribuzione in via originaria di ruoli funzionali tipizzati dalla legge, dalla delega di funzioni, che determina un decentramento derivato di poteri decisionali. V. anche Cassazione penale, sez. IV, 26 aprile 2017, n. 24958, su *dejure.it*, ove si afferma che la mera designazione del responsabile del servizio di prevenzione e protezione non costituisca una delega di funzioni e non sia dunque sufficiente a sollevare il datore di lavoro ed i dirigenti dalle rispettive responsabilità in tema di violazione degli obblighi dettati per la prevenzione degli infortuni sul lavoro.

<sup>53</sup> Cfr. GARGANI (2017), p. 521.

<sup>54</sup> Sul tema delle incompetenze tecnico-scientifiche del vertice dell'impresa, cfr. KELLER (2018), p. 113 ss.

alla segmentazione dei poteri decisionali. Con tale strumento si prevede, infatti, in modo espresso la possibilità, per i contitolari di un medesimo trattamento, di determinare mediante un accordo le aree di rispettiva competenza e, dunque, di rispettiva responsabilità: tale istituto si rivela, dunque, di particolare interesse, nella prospettiva che ci occupa, poiché attribuisce rilievo giuridico all'eventuale coinvolgimento di più soggetti nella determinazione delle finalità e dei mezzi del trattamento, e, dunque, risponde all'esigenza di saper distinguere tra le singole posizioni *funzionali* all'interno dell'organizzazione, «evitando irragionevoli "livellamenti" tra le incombenze dei soggetti» chiamati singolarmente a rivestirle<sup>55</sup>.

## 4. Conclusioni.

Il sensibile mutamento di prospettiva adottato con il *Regolamento Generale sulla Protezione dei Dati* è, dunque, destinato indubbiamente a irradiare i suoi riflessi anche in materia penale: ciò, non soltanto in conseguenza dell'ampliamento dell'oggetto e delle funzioni della tutela, nell'era della *datification*<sup>56</sup>, ma anche in virtù del dichiarato cambiamento di approccio, da una disciplina incentrata sui diritti dell'interessato – quale era l'originaria direttiva 95/46 – alla attuale «tutela preventiva fondata sulla strutturale e dinamica responsabilizzazione della filiera soggettiva coinvolta nel trattamento dei dati personali»<sup>57</sup>.

Pertanto, come si è detto, anche in tale settore acquisisce una crescente importanza il fattore organizzativo, attesa la rilevanza cruciale assunta dall'adozione di modelli organizzativi funzionali alla prevenzione degli illeciti provenienti non già dall'esterno, ma anche dall'interno dell'organizzazione, mediante, per l'appunto, controlli e processi di formazione che assicurino il rispetto della normativa – e, dunque, la prevenzione del rischio-illecito – da parte dei dipendenti dell'impresa<sup>58</sup>.

L'analisi della nuova disciplina in materia di protezione di dati personali è occasione, dunque, per formulare talune considerazioni di carattere più ampio, relative al tema, ben più vasto, dei rapporti tra diritto, responsabilità e tecnica, in connessione con la complessità delle organizzazioni.

Sembra, infatti, che a fronte della crescente importanza di una tutela (anche penale) dei dati personali e dell'integrità dei sistemi tecnologici nella società dell'informazione, anche il settore informatico-digitale possa aggiungersi a quei campi in cui la preponderanza della tecnica può portare a un problematico disallineamento tra poteri, doveri e responsabilità, disallineamento che, invece, proprio uno strumento quale la delega di funzioni potrebbe contribuire a risolvere, valorizzando competenze differenziate<sup>59</sup>.

Invero, nella prospettiva dei rapporti tra tecnica e diritto, se l'affiancamento di prescrizioni giuridiche e prescrizioni tecniche nel tessuto del *Regolamento Generale sulla Protezione dei Dati* sembra non aver attribuito interamente «al detentore del potenziale pericoloso la potestà decisionale sulla misura del rischio consentito»<sup>60</sup> e sugli strumenti con il quale contrastarlo, tuttavia l'indissolubile integrazione tra dato tecnico e norma giuridica accresce la complessità dei rapporti tra i soggetti detentori del potere decisionale-organizzativo e le figure che, invece, apportano un sapere tecnico nelle procedure di gestione del rischio.

A prescindere dal dato normativo, dunque, è evidente che anche con riguardo alla tutela dei dati personali dovranno essere opportunamente valorizzati quegli atti organizzativi che determinino il coinvolgimento cooperativo di soggetti diversi nell'adempimento degli obblighi di tutela prescritti dal *Regolamento*<sup>61</sup>, al fine di ripartire le responsabilità penali ricondu-

<sup>55</sup> In tal senso DE FRANCESCO (2012), p. 3929.

<sup>56</sup> Per questo concetto si rinvia a CALZOLAIO (2017), p. 598.

<sup>57</sup> Cfr. ancora CALZOLAIO (2017), p. 614.

<sup>58</sup> Come si è detto, riprendendo la classificazione di GARGANI (2017), p. 515, si potrebbe, dunque, ritenere che con il *GDPR* si configurino sia forme di prevenzione del rischio *lecito*, sia forme di prevenzione del rischio *illecito*.

<sup>59</sup> Competenze che, nell'era della "tecnicizzazione", si trasformano in uno strumento di potere, per cui v. CALZOLAIO (2017), *passim*: «l'evoluzione tecnica (tecnicizzazione) aveva la forza di incrementare tutti i presupposti dell'universo dell'esperienza, con ciò modificando le dinamiche del potere come mezzo di comunicazione (e della struttura sociale)».

<sup>60</sup> A tal proposito, v. STELLA (2003), p. 57.

<sup>61</sup> Cfr. GARGANI (2017), p. 520. V. anche la soluzione adottata da Cassazione penale, sez. IV, 30 settembre 2015, n. 10177, su *dejure.it*, ove si è ritenuto che l'apporto fornito dal responsabile del servizio di prevenzione e protezione sia parte inscindibile di una procedura complessa che sfocia nelle scelte operative compiute dal titolare dell'impresa, cosicché la sua attività possa senz'altro rilevare ai fini della spiegazione causale dell'evento illecito, e anche la pronuncia di Cassazione penale, sez. IV, 23 novembre 2012, n. 49821, su *dejure.it*, secondo cui il responsabile

cendo ad unità tale moltiplicazione dei garanti.

---

## Bibliografia

- ALESSANDRI (2010): *Diritto penale e attività economiche* (Bologna, Il Mulino).
- ID. (2005): “Attività d’impresa e responsabilità penali”, *Riv. it. dir. proc. pen.*, 2, pp. 534 ss.
- ALESSANDRI e SEMINARA (2018): *Diritto penale commerciale*, Vol. 1 (Torino, Giappichelli).
- AMBROSETTI, MEZZETTI, RONCO (2012): *Diritto penale dell’impresa* (Bologna, Zanichelli).
- BASILE (2018): *Consiglio tecnico e responsabilità penale: il concorso del professionista tramite azioni ‘neutrali’* (Milano, Giuffrè).
- BISORI (1997): “L’omesso impedimento del reato altrui nella dottrina e nella giurisprudenza italiana”, *Rivista italiana di diritto e procedura penale*, pp. 1340 ss.
- BLAIOTTA (1999): “Le fattispecie penali introdotte dalla legge sulla privacy”, *Cassazione penale*, 5, pp. 1642 ss.
- CALZOLAIO (2017): “Protezione dei dati personali (dir. pubbl.)”, *Digesto delle discipline pubblicistiche*, Agg., pp. 594 ss. (Torino, UTET).
- CENTONZE (2009): *Controlli societari e responsabilità penale* (Milano, Giuffrè).
- CONSULICH (2015): “Vigilantes puniri possunt. I destini dei componenti dell’organismo di vigilanza tra doveri impeditivi e cautele relazionali”, *Rivista trimestrale di diritto penale dell’economia*, pp. 425 ss.
- D’AGOSTINO (2019): “La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101”, *Archivio penale*, 1.
- D’ALESSANDRO (2016): “Delega di funzioni (diritto penale)”, *Enciclopedia del diritto*, Annali, IX, pp. 241 ss. (Milano, Giuffrè).
- DE FRANCESCO (2012): “Il concorso di persone e il dogma causale: rilievi critici e proposte alternative”, *Cassazione penale*, 11, pp. 3913 ss.
- GARGANI (2017): “Posizioni di garanzia nelle organizzazioni complesse: problemi e prospettive”, *Rivista trimestrale di diritto penale dell’economia*, 3-4, pp. 508 ss.
- GIUNTA (2006), “Controllo e controllori nello specchio del diritto penale societario”, *Rivista trimestrale di diritto penale dell’economia*, pp. 597 ss.
- KELLER (2018): “L’irrilevanza penale delle (in)competenze tecnico-scientifiche del datore di lavoro indispensabili per la valutazione dei rischi”, *Diritto penale contemporaneo*, 10, pp. 113 ss.
- LABIANCA (2019): “Il sistema delle tutele nel Regolamento Europeo n. 679/2016 sulla protezione dei dati personali”, in CADOPPI, CANESTRARI, MANNA, PAPA, *Cybercrime*, (Milano, UTET), pp. 977 ss.
- LEONCINI (1999): *Obbligo di attivarsi, obbligo di garanzia e obbligo di sorveglianza* (Torino, Giappichelli).
- LUBERTO (2019): “Data breach e delitto dell’art. 168 D.Lgs. n. 196/2003”, in CADOPPI, CANESTRARI, MANNA, PAPA, *Cybercrime*, (Milano, UTET), pp. 942 ss.

---

del servizio di prevenzione e protezione può diventare titolare di una posizione di garanzia penalmente rilevante se coinvolto direttamente nell’esercizio di poteri gestionali.

MANES, MAZZACUVA (2019): “GDPR e nuove disposizioni penali del Codice privacy”, *Diritto penale e processo*, 2, pp. 171 ss.

MANNA, DI FLORIO (2019): “Riservatezza e diritto alla *privacy*”, in CADOPPI, CANESTRARI, MANNA, PAPA, *Cybercrime*, (Milano, UTET), pp. 891 ss.

MASSARO (2013): *La responsabilità colposa per omesso impedimento di un fatto illecito altrui* (Napoli, Jovene).

NAUWELAERTS (2018): *Data Protection & Privacy* (Londra, Law Business Research).

PICOTTI (2013): “La tutela penale della persona e le nuove tecnologie dell’informazione”, in ID., *Tutela penale della persona e nuove tecnologie*, (Padova, Cedam), pp. 29 ss.

PIERGALLINI (2017): “Colpa (diritto penale)”, *Enciclopedia del diritto*, Annali, X, pp. 222 ss.

PROVOLO (2019): “Il sistema sanzionatorio del novellato Codice della *privacy* e la tutela penale *patchwork* dei dati genetici e dei dati biometrici”, *Rivista trimestrale di diritto penale dell’economia*, 2, pp. 242 ss.

RESTA (2019): “I reati in materia di protezione dei dati personali”, in CADOPPI, CANESTRARI, MANNA, PAPA, *Cybercrime*, (Milano, UTET), pp. 1019 ss.

RICCI (2018): “Trattamento di dati sensibili e principio di responsabilizzazione”, *Giurisprudenza italiana*, 12, 2641 ss.

STELLA (2003): “La costruzione giuridica della scienza: sicurezza e salute negli ambienti di lavoro”, *Rivista italiana di diritto e procedura penale*, 1, 55 ss.

TORRE (2004), “La gestione del rischio nella disciplina del trattamento dei dati personali”, in PICOTTI, *Il diritto penale dell’informatica nell’epoca di internet*, (Padova, Cedam), pp. 237 ss.

VOIGT e VON DEM BUSSCHE (2017): *The EU General Data Protection Regulation (GDPR)* (Cham, Springer).

WORKING PARTY ARTICLE 29 (2017): *Guidelines on Data Protection Officers (‘DPOs’)*, *ec.europa.eu*.



Diritto Penale Contemporaneo

R I V I S T A   T R I M E S T R A L E

---

REVISTA TRIMESTRAL DE DERECHO PENAL  
A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

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