

CJN

# Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL  
A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

4.3% | PORT:A | NETWORK | SETTING | HELP?

1/2023

## 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 EDITORS

Carlo Bray, Silvia Bernardi

## EDITORIAL STAFF

Enrico Andolfatto, Enrico Basile, Emanuele Birritteri, Javier Escobar Veas,

Stefano Finocchiaro, Alessandra Galluccio, Elisabetta Pietrocarlo, Rossella Sabia,

Tommaso Trinchera, Maria Chiara Ubiali

## EDITORIAL ADVISORY BOARD

Rafael Alcacer Guirao, Alberto Alessandri, Silvia Allegrezza, Chiara Amalfitano, Giuseppe Amarelli, Ennio Amodio, Coral Arangüena Fanego, Lorena Bachmaier Winter, Roberto Bartoli, Fabio Basile, Hervé Belluta, Alessandro Bernardi, Carolina Bolea Bardon, Manfredi Bontempelli, Nuno Brandão, David Brunelli, Silvia Buzzelli, Alberto Cadoppi, Pedro Caeiro, Michele Caianiello, Lucio Camaldo, Stefano Canestrari, Francesco Caprioli, Claudia Marcela Cárdenas Aravena, Raúl Carnevali, Marta Cartabia, Elena Maria Catalano, Mauro Catenacci, Antonio Cavaliere, Massimo Ceresa Gastaldo, Mario Chiavario, Federico Consulich, Mirentxu Corcoy Bidasolo, Roberto Cornelli, Cristiano Cupelli, Norberto Javier De La Mata Barranco, Angela Della Bella, Cristina de Maglie, Gian Paolo Demuro, Miguel Díaz y García Conlledo, Francesco D'Alessandro, 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 Caverro, 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 Lascuráin 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 Masera, Jean Pierre Matus Acuña, Anna Maria Maugeri, Oliviero Mazza, Iván Meini, Alessandro Melchionda, Chantal Meloni, Melissa Miedico, Vincenzo Militello, Fernando Miró Linares, Vincenzo Mongillo, Renzo Orlandi, Magdalena Ossandón W., Francesco Palazzo, Carlenrico Paliero, Michele Papa, Raphaële Parizot, Claudia Pecorella, Marco Pelissero, Lorenzo Picotti, Carlo Piergallini, Paolo Pisa, Oreste Pollicino, Domenico Pulitanò, Serena Quattrococo, Tommaso Rafaraci, Paolo Renon, Lucia Risicato, Mario Romano, Maria Ángeles Rueda Martín, Carlo Ruga Riva, Stefano Ruggeri, Francesca Ruggieri, Dulce Maria Santana Vega, Marco Scoletta, Sergio Seminara, Paola Severino, Nicola Selvaggi, Rosaria Sicurella, Jesús Maria Silva Sánchez, Carlo Sotis, Giulio Ubertis, Inma Valeije Álvarez, Antonio Vallini, Gianluca Varraso, Vito Velluzzi, Paolo Veneziani, John Vervaele, Daniela Vigoni, Costantino Visconti, Javier Wilenmann von Bernath, Francesco Zacchè, Stefano Zirulia

Editore Associazione "Progetto giustizia penale", c/o Università degli Studi di Milano,  
Dipartimento di Scienze Giuridiche "C. Beccaria" - Via Festa del Perdono, 7 - 20122 MILANO - c.f. 97792250157  
ANNO 2023 - 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.

I contributi da sottoporre alla Rivista possono essere inviati al seguente indirizzo mail: [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](#)).

<p>INTELLIGENZA ARTIFICIALE E DIRITTO PENALE</p> <p><i>INTELIGENCIA ARTIFICIAL Y DERECHO PENAL</i></p> <p><i>ARTIFICIAL INTELLIGENCE AND CRIMINAL LAW</i></p>	<p><b><i>Criminal compliance e nuove tecnologie</i></b> 1</p> <p><b><i>Criminal compliance y nuevas tecnologías</i></b></p> <p><b><i>Criminal Compliance and New Technologies</i></b></p> <p>Luca D'Agostino</p> <hr/> <p><b><i>La responsabilità penale del produttore di sistemi di intelligenza artificiale</i></b> 26</p> <p><b><i>La responsabilidad penal del fabricante de sistemas de inteligencia artificial</i></b></p> <p><b><i>The Criminal Liability of Artificial Intelligence System Manufacturers</i></b></p> <p>Beatrice Fragasso</p> <hr/> <p><b><i>AI and Criminal Liability. Algorithmic Error and Human Negligence in the Context of the European Regulation</i></b> 46</p> <p><b><i>IA e responsabilità penale. Errore dell'algoritmo e colpa della persona fisica nel contesto della regolamentazione europea</i></b></p> <p><b><i>IA y Responsabilidad Penal. Error de algoritmo y culpa de la persona natural en el contexto de la regulación europea.</i></b></p> <p>Marta Giuca</p> <hr/> <p><b><i>La responsabilità penale al tempo di ChatGPT</i></b> 70</p> <p><b><i>La responsabilidad penal en la era de ChatGPT</i></b></p> <p><b><i>Criminal Liability in the Era of ChatGPT</i></b></p> <p>Leonardo Romanò</p> <hr/>
<p>SPECIALE SU "SICUREZZA DELLO STATO E POTERI INVESTIGATIVI PARALLELI"</p> <p><i>ESPECIAL SOBRE "SEGURIDAD DEL ESTADO Y FACULTADES INVESTIGATIVAS PARALELAS"</i></p> <p><i>SPECIAL ON "STATE SECURITY AND PARALLEL INVESTIGATIVE POWERS"</i></p>	<p><b><i>Speciale su "Sicurezza dello Stato e poteri investigativi paralleli".</i></b> 92</p> <p><b><i>Premessa</i></b></p> <p><b><i>Especial sobre "Seguridad del Estado y facultades investigativas paralelas".</i></b></p> <p><b><i>Premisa</i></b></p> <p><b><i>Special on "State security and parallel investigative powers".</i></b></p> <p><b><i>Introduction</i></b></p> <p>Donatella Curtotti</p> <hr/> <p><b><i>Agenzia per la cybersicurezza nazionale, sicurezza della Repubblica e investigazioni dell'Autorità giudiziaria</i></b> 97</p> <p><b><i>Agencia Nacional de Ciberseguridad, Seguridad de la República italiana e investigación judicial</i></b></p> <p><b><i>National Cybersecurity Agency, Security of Italian Republic and Judicial Investigation</i></b></p> <p>Federico Niccolò Ricotta</p>

	<b>Le indagini d'intelligence e gli strumenti d'intercettazione preventiva</b>	114
	<i>Investigaciones de inteligencia y herramientas de interceptación preventiva</i>	
	<i>Intelligence Investigations and Preventive Interception Tools</i>	
	Wanda Nocerino	
	<b>Le inchieste dell'agenzia nazionale per la sicurezza del volo e i limiti all'attività della polizia giudiziaria</b>	134
	<i>Las investigaciones de la Agencia de Seguridad Aeronáutica y los límites a la actividad de la policía judicial</i>	
	<i>Investigations by the National Agency for Flight Safety and the Limits to the Activity of the Judicial Police</i>	
	Ottavia Murro	
	<b>Securitizzazione dell'Unione europea e poteri concorrenti. Dall'investigazione, alla prevenzione, all'osservazione</b>	145
	<i>Securitización y competencias concurrentes en la Unión Europea. De la investigación a la observación y prevención</i>	
	<i>Securitization and Competing Powers in the European Union. From Investigation to Observation and Prevention</i>	
	Angela Procaccino	
<i>IL FOCUS SU...</i>	<b>Il rinvio pregiudiziale in ambito penale e i problemi posti dalle sentenze interpretative della Corte di Giustizia</b>	172
<i>FOCUS SOBRE...</i>	<i>La remisión prejudicial en materia penal y los problemas que generan las sentencias interpretativas del Tribunal de Justicia</i>	
<i>FOCUS ON...</i>	<i>The Preliminary Reference in Criminal Matters and the Issues Raised by Interpretative Judgments of the Court of Justice</i>	
	Alessandro Bernardi	
	<b>The Crime of Money Laundering: A Touchstone for The Principles of Il Manifesto del diritto penale liberale e del giusto processo</b>	213
	<i>Il reato di riciclaggio: un banco di prova per i principii del Manifesto del diritto penale liberale e del giusto processo</i>	
	<i>El delito de lavado de activos: una prueba para los principios del Manifesto del derecho penal liberal y del debido proceso</i>	
	Matthias Jahn, Federica Helferich	
	<b>"Gimme Shelter": The Right to Silence for Silenced Migrant Victims</b>	227
	<i>"Gimme Shelter": il diritto al silenzio per le vittime migranti silenziate</i>	
	<i>"Gimme Shelter": el derecho al silencio por las víctimas migrantes silenciadas</i>	
	Sara Bianca Taverriti	

SPECIALE SU “SICUREZZA DELLO STATO  
E POTERI INVESTIGATIVI PARALLELI”

*ESPECIAL SOBRE “SEGURIDAD DEL ESTADO  
Y FACULTADES INVESTIGATIVAS PARALELAS”*

*SPECIAL ON “STATE SECURITY  
AND PARALLEL INVESTIGATIVE POWERS”*

- 92 **Speciale su “Sicurezza dello Stato e poteri investigativi paralleli”. Premessa**  
*Especial sobre “Seguridad del Estado y facultades investigativas paralelas”. Premisa*  
*Special on “State security and parallel investigative powers”. Introduction*  
Donatella Curtotti
- 97 **Agenzia per la cybersicurezza nazionale, sicurezza della Repubblica  
e investigazioni dell’Autorità giudiziaria**  
*Agencia Nacional de Ciberseguridad, Seguridad de la República italiana  
e investigación judicial*  
*National Cybersecurity Agency, Security of Italian Republic  
and Judicial Investigation*  
Federico Niccolò Ricotta
- 114 **Le indagini d’intelligence e gli strumenti d’intercettazione preventiva**  
*Investigaciones de inteligencia y herramientas de interceptación preventiva*  
*Intelligence Investigations and Preventive Interception Tools*  
Wanda Nocerino
- 134 **Le inchieste dell’agenzia nazionale per la sicurezza del volo e i limiti all’attività della polizia  
giudiziaria**  
*Las investigaciones de la Agencia de Seguridad Aeronáutica y los límites a la actividad de la policía judicial*  
*Investigations by the National Agency for Flight Safety and the Limits to the Activity of the Judicial Police*  
Ottavia Murro
- 145 **Securitizzazione dell’Unione europea e poteri concorrenti.  
Dall’indagine, alla prevenzione, all’osservazione**  
*Securitización y competencias concurrentes en la Unión Europea.*  
*De la investigación a la observación y prevención*  
*Securitization and Competing Powers in the European Union.*  
*From Investigation to Observation and Prevention*  
Angela Procaccino

# Agenzia per la *cybersicurezza* nazionale, sicurezza della Repubblica e investigazioni dell’Autorità giudiziaria

*Agencia Nacional de Ciberseguridad, Seguridad de la República italiana e investigación judicial*

*National Cybersecurity Agency, Security of Italian Republic and Judicial Investigation*

FEDERICO NICCOLÒ RICOTTA  
*Assegnista di ricerca nell’Università degli Studi di Foggia*  
*federico.ricotta@unifg.it*

REATI INFORMATICI,  
INDAGINI PRELIMINARI

DELITOS INFORMÁTICOS,  
INVESTIGACIONES PRELIMINARES

CYBERCRIMES,  
PRE-TRIAL INVESTIGATION

---

---

## ABSTRACTS

Il contributo analizza il ruolo e le funzioni della nuova Agenzia per la *cybersicurezza*, con particolare riferimento al rango della sicurezza cibernetica, all’applicabilità della disciplina prevista per il sistema di informazione per la sicurezza della Repubblica, alle indagini di sicurezza e alle possibili sovrapposizioni con i poteri dell’Autorità Giudiziaria.

El artículo analiza el papel y las funciones de la nueva Agencia de Ciberseguridad, con especial referencia al rango de la ciberseguridad, la aplicabilidad de la normativa prevista para el sistema de información de seguridad de la República, las investigaciones de seguridad, y los posibles solapamientos con las competencias de la Autoridad Judicial.

The paper analyzes role and functions of the new Cybersecurity Agency, with particular reference to the rank of cybersecurity, the applicability of the regulations provided for the Republic's security information system, security investigations, and possible overlaps with the powers of the Judicial Authority.

## SOMMARIO

1. Introduzione – 2. Le istituzioni a salvaguardia della sicurezza cibernetica – 3. Sicurezza nazionale, architettura nazionale per la cybersicurezza e Sistema di informazione per la sicurezza della Repubblica – 4. L’Agenzia per la cybersicurezza nazionale: un’agenzia di *intelligence* oppure no? – 5. *Segue*. L’inapplicabilità della speciale disciplina in materia di attività di informazione per la sicurezza della Repubblica – 6. *Segue*. La comunicazione della notizia di reato – 7. – I poteri investigativi dell’Agenzia per la cybersicurezza nazionale e le indagini dell’autorità giudiziaria – 8. Cenni sulla migrazione dei risultati dell’inchiesta amministrativa e sull’art. 220 disp. att. c.p.p. – 9. La concorrenza investigativa.

## 1.

## Introduzione.

L’incremento delle minacce nel dominio cibernetico e la complicazione del quadro-geopolitico globale hanno accresciuto l’esposizione della Repubblica Italiana al pericolo di attacchi di natura informatica alle infrastrutture critiche, ai servizi e alle funzioni essenziali. Le principali capacità nazionali di risposta, analisi, vigilanza e prevenzione nel dominio cibernetico<sup>1</sup>, transitoriamente affidate alle competenze del Sistema di informazione per la Sicurezza della Repubblica, sono oggi trasferite all’Agenzia per la cybersicurezza nazionale (ACN)<sup>2</sup>, alla quale la legge attribuisce un complesso di poteri certificativi, investigativi e sanzionatori necessari al perseguimento della propria missione istituzionale.

L’assetto istituzionale e normativo in materia di cybersicurezza solleva almeno tre ordini di quesiti. Il primo riguarda la natura dell’Agenzia cyber: c’è da chiedersi se l’Agenzia sia un’agenzia di *intelligence*; e, in caso di risposta positiva, quali siano le regole da applicare, tenendo conto sia delle garanzie previste dalla legge 3 agosto 2007 n. 124 (la legge sul sistema di informazione per la sicurezza della Repubblica e sulla nuova disciplina del segreto di Stato), sia di quelle stabilite dal codice di procedura penale. Inoltre, sul presupposto che ogni attacco informatico è potenzialmente un crimine, occorre ulteriormente domandarsi se i poteri investigativi attribuiti all’Agenzia possano innescare sovrapposizioni con quelli dell’autorità giudiziaria.

## 2.

## Le istituzioni a salvaguardia della sicurezza cibernetica.

L’attuale disciplina in materia di sicurezza cibernetica è contenuta essenzialmente in tre principali testi normativi che definiscono il sistema a livello europeo e nazionale<sup>3</sup>: la direttiva (UE)2016/1148 del 6 luglio 2016, la cd. NIS – “*Network and information security*”, per l’adozione di misure al fine raggiungere elevati standard nella sicurezza delle reti e dei sistemi informativi all’interno dell’Unione e recepita in Italia dal d.lgs. 18 maggio 2018, n. 65<sup>4</sup>; il decreto-legge 21 settembre 2019 n. 105, così come convertito dalla legge 18 novembre 2019, n. 133, ed i successivi decreti attuativi<sup>5</sup>, che hanno introdotto il perimetro nazionale di sicurezza cibernetica; il decreto-legge 14 giugno 2021 n. 82, convertito con modificazioni con la legge 4 agosto 2021 n. 109<sup>6</sup>, che ha definito l’attuale architettura nazionale di cybersicurezza,

<sup>1</sup> Lo “spazio cibernetico” è definito come «l’insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi. Esso dunque comprende internet, le reti di comunicazione, i sistemi su cui poggiano i processi informatici di elaborazione dati e le apparecchiature mobili dotate di connessione di rete» cit. PRESIDENZA DEL CONSIGLIO DEI MINISTRI (2013), p. 10.

<sup>2</sup> Ai sensi dell’art. 1 del decreto-legge 14 giugno 2021 n. 82, convertito con modificazioni dalla l. 4 agosto 2021, n. 109, per cybersicurezza deve intendersi l’insieme delle attività necessarie alla protezione dalle minacce informatiche di reti, sistemi informativi, servizi informativi e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l’integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell’interesse nazionale nello spazio cibernetico.

<sup>3</sup> Completano il quadro delle disposizioni UE rilevanti il Regolamento UE 2019/881, il cd. “*Cybersecurity Act*”, che ha portato all’istituzione dell’Autorità Nazionale di Certificazione della Cybersicurezza la Direttiva n. 2018/1972, il cd. Codice Europeo delle Comunicazioni Elettroniche, recepito nell’ordinamento italiano dal d. lgs. 8 novembre 2021, n. 207, che ha modificato le disposizioni introdotte nel d.lgs. 259/2003. Per un approfondimento v. CAROTTI (2020), p. 629 ss.; RENZI (2021), p. 538 ss.

<sup>4</sup> La NIS è stata sostituita dalla cd. NIS 2, la Direttiva (UE) 2022/2555 che ha ulteriormente innalzato i presidi necessari all’identificazione, la valutazione e la mitigazione del rischio cibernetico.

<sup>5</sup> Così come interpolato dal d.l. n. 162/2019 in materia di proroga dei termini e altre disposizioni sulla pubblica amministrazione. In attuazione del d.l. n. 105/2019 sono stati adottati il DPCM 30 luglio 2020, n. 131, concernente criteri e modalità per l’individuazione dei soggetti inclusi nel perimetro nazionale di sicurezza cibernetica, e il DPCM 14 aprile 2021, n. 81 sulle modalità per la notifica nel caso di incidenti riguardanti beni ITC. Si veda in particolare il dossier del servizio studi del Senato della Repubblica, *Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*, 11 novembre 2019, disponibile su [documenti.camera.it](https://www.camera.it/documenti).

<sup>6</sup> Il d.l. n. 105/2019, in particolare, individua le amministrazioni pubbliche, enti ed operatori pubblici e privati che hanno sede nel territorio

provvedendo al riordino e all'accentramento delle competenze in seno all'Agenzia per la cybersicurezza nazionale.

Più specificamente gli articoli 1, 2, 3 e 4 del d.l. n. 82/2021 definiscono la struttura del sistema nazionale di sicurezza cibernetica, vale a dire il complesso di organi e strutture, tra di loro autonomi, che si coordinano e interagiscono fra loro per assolvere all'insieme delle determinazioni necessarie alla difesa e alla resilienza digitale dello Stato nel dominio cibernetico.

Al vertice del sistema è posto il Presidente del Consiglio dei ministri, a cui la legge attribuisce l'alta direzione e la responsabilità generale delle politiche di cybersicurezza<sup>7</sup>, con la facoltà di delegare le funzioni che non gli sono conferite in via esclusiva all'Autorità Delegata per il Sistema di informazione per la sicurezza della Repubblica. Presso la Presidenza del Consiglio è stato istituito il Comitato interministeriale per la cybersicurezza (CIC), l'organismo cui sono attribuite funzioni di vigilanza, consulenza e proposta nell'ambito delle politiche in ambito cibernetico<sup>8</sup>; infine, il sistema si completa con l'Agenzia per la cybersicurezza nazionale e, in seno ad essa, il Nucleo per la cybersicurezza e gestione della crisi<sup>9</sup> ed il *Computer Security Incident Response Team Italia*, il CSIRT.

### 3. Sicurezza nazionale, architettura nazionale per la cybersicurezza e Sistema di informazione per la sicurezza della Repubblica.

L'adozione del d.l. 14 giugno 2021 n. 82, così come convertito in legge, ha rinnovato l'attuale architettura nazionale di sicurezza cibernetica su quattro grandi pilastri di competenze tra loro diversificate ma comunicanti<sup>10</sup>: la cybersicurezza e la resilienza nello spazio cibernetico, affidata all'Agenzia per la cybersicurezza nazionale; la raccolta e l'analisi informativa, affidata al Sistema di informazione per la sicurezza della Repubblica; la difesa e la sicurezza militare dello Stato, affidata al Ministero della Difesa; la prevenzione e il contrasto dei reati, di competenza delle forze di polizia e dell'autorità giudiziaria.

Prima della definizione del perimetro di sicurezza nazionale e dell'istituzione dell'Agenzia *cyber*<sup>11</sup>, la tutela della Repubblica dall'imperversare delle minacce nel dominio cibernetico era affidata all'attività istituzionale svolta dal Dipartimento delle Informazioni per la sicurezza, il DIS, l'organo di coordinamento del Sistema di informazione per la sicurezza della Repubblica, che disponeva di risorse e capacità adeguate all'incarico<sup>12</sup>: un ruolo di supplenza che il DIS ha transitoriamente mantenuto sino all'entrata in vigore della nuova architettura nazionale di cybersicurezza<sup>13</sup>.

nazionale che rientrano nel perimetro di sicurezza, e che per questo sono tenuti al rispetto di obblighi e delle misure in funzione di tutela della sicurezza nazionale (v. in tal senso art. 1 comma 2 del menzionato decreto-legge).

<sup>7</sup>Le attribuzioni in materia cyber si aggiungono all'alta direzione e alla responsabilità generale della politica dell'informazione per la sicurezza che l'art. 1, c. 1, lett. a della legge n. 124/2007 già conferisce al Presidente del Consiglio dei Ministri.

<sup>8</sup>Fanno parte del CIC il Presidente del Consiglio (che lo presiede); l'Autorità delegata, ove istituita; e, secondo la nomenclatura richiamata dalla legge, il Ministro degli affari esteri e della cooperazione internazionale; il Ministro dell'interno; il Ministro della giustizia; il Ministro della difesa; il Ministro dell'economia e delle finanze; il Ministro dello sviluppo economico; il Ministro della transizione ecologica; il Ministro dell'università e della ricerca; il Ministro delegato per l'innovazione tecnologica e la transizione digitale; il Ministro delle infrastrutture e della mobilità sostenibili.

<sup>9</sup>Il nucleo è presieduto dal direttore o dal vicedirettore generale dell'ACN ed è composto dal Consigliere militare del Presidente del Consiglio, e da un rappresentante di DIS, AISI, AISE, di ciascuno dei ministeri del CIC e del Dipartimento della protezione civile. Limitatamente alla trattazione di informazioni classificate, anche da un rappresentante dell'Ufficio centrale per la segretezza (istituito presso il DIS, ai sensi dell'articolo 9 della legge n. 124 del 2007).

<sup>10</sup>Il concetto di "difesa" cyber, che allude al complesso delle attività che insistono sulla preparazione delle capacità di natura militare e alla difesa dalle aggressioni di mano straniera e statale, è oggi aggiornato e incorporato in quello concettualmente più ampio di "resilienza cibernetica", che come si vedrà a brevissimo sintetizza un novero di attribuzioni e responsabilità *urbi et orbi* deputate al rafforzamento delle capacità nazionali di resistenza cibernetica, negli ambiti essenziali per gli interessi strategici della nazione, in termini non soltanto di risposta all'incidente, ma di prevenzione, sviluppo tecnologico, formazione ed informazione negli ambiti pubblici e privati. In particolare, in AZZARONE (2015c), p. 86 s. è contenuta un'ampia analisi della galassia delle possibili minacce nel dominio cyber, come in materia di comunicazioni mobili, telefonia Voip, *open source software* (Oss), infrastruttura bitcoin, sistemi satellitari, *Internet of things* e automobili di nuova generazione.

<sup>11</sup>DE GENNARO (2011); AZZARONE (2014a), pp. 62 – 76; AZZARONE (2014b), pp. 36 – 47; AZZARONE (2014c); AZZARONE (2015a), pp. 88 – 98; AZZARONE (2015b), pp. 124 – 132; AZZARONE (2015c), pp. 84 – 94.

<sup>12</sup>Dal canto suo, il comparto di informazione per la sicurezza della Repubblica già da tempi non sospetti ha colto la rilevanza del dominio cyber tra le attività strategiche di interesse per la sicurezza nazionale, potenziando le proprie capacità anche in termini di cyber-intelligence (o CYBINT) e quindi di raccolta e analisi informativa pensata e adattata alle specificità del dominio operativo cibernetico CALIGURI (2016), p. 23 s.; GORI (2016), p. 87 s.

<sup>13</sup>Già la strategia nazionale per la sicurezza dello spazio cibernetico, delineata con il Decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013, definiva il quadro strategico per individuare i profili di minaccia per i sistemi e le reti di interesse nazionale, distribuendo

In effetti, la minaccia *cyber* ha da sempre avuto l'attitudine a incidere in modo trasversale in tutti i settori che la legge n. 124/2007 definisce come di interesse istituzionale dell'attività dell'*intelligence*, racchiusi nel prisma del concetto di sicurezza nazionale<sup>1418</sup>. Sicché, da un punto di vista di sistema, la considerazione più rilevante da cui partire è il rango della sicurezza *cyber* e la sua appartenenza allo spettro delle responsabilità di Alta direzione delle politiche di sicurezza nazionale che sono attribuite in via ordinaria al Presidente del Consiglio dei ministri<sup>15</sup>.

Non c'è dubbio che la sicurezza nel dominio cibernetico sia una delle espressioni del moderno concetto di sicurezza nazionale<sup>16</sup>, con il quale individuamo quel novero di valori indispensabili sui quali si basa la stessa sopravvivenza della Repubblica come comunità di istituzioni e di cittadini e quelle indefettibili necessità ultra-individuali legate al mantenimento delle condizioni essenziali per tenere una nazione unita e proteggerne lo sviluppo<sup>17</sup>.

Questa modernità della sicurezza nazionale si coglie in ragione del fatto che, a fianco delle esigenze più tradizionali quali la difesa dello Stato democratico e delle istituzioni poste dalla Costituzione a suo fondamento, sono state individuate nuove aree di intervento, quali l'economia, l'industria, l'energia o la tecnologia, segnando il passaggio ad una nuova era<sup>18</sup>: quella dell'emancipazione da una dimensione della sicurezza che era circoscritta allo Stato-apparato, dove è lo Stato stesso ad essere il monopolista dei beni giuridici da proteggere, ad una sicurezza che abbraccia lo Stato-comunità e tutte le sue plurime, trasversali, espressioni in campo sociale, industriale, economico e scientifico, e, da ultimo, nondimeno cibernetico.

Tanto è vero che il pregiudizio alla sicurezza nazionale è stato di recente cristallizzato nell'art. 1 del D.P.C.M. n. 131 del 20 luglio 2020, che lo declina come “danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale”.

Ad una nozione pluralista e multiforme della sicurezza nazionale corrisponde, nei fatti, una certa omogeneità nella struttura delle articolazioni deputate a garantirla: l'architettura *cyber* sembra essere stata mutuata da quella del Sistema di informazione per la sicurezza della Repubblica, così come definito dalla legge n. 124/2007<sup>19</sup>. In entrambi i casi l'organo apicale, centro delle responsabilità e dei poteri in materia di sicurezza della Repubblica, è il Presidente del Consiglio, il “crocevia istituzionale” dell'intero sottosistema di organismi e di autorità, con il potere di impartire direttive per la sicurezza (anche *cyber*) ed emanare disposizioni per l'organizzazione e il funzionamento delle agenzie; l'autorità delegata per il Sistema di informazione può ricevere le deleghe presidenziali in materia di sicurezza cibernetica; anche per il sistema *cyber* è prevista la vigilanza del Comitato parlamentare per la sicurezza della Repubblica (il COPASIR)<sup>20</sup>, c'è il Comitato interministeriale e, infine, mentre per il comparto di sicurezza ci sono due agenzie con competenze all'interno (AISI) ed all'esterno (AISE) dei confini della Repubblica, per la sicurezza cibernetica c'è l'ACN che assolve le principali funzioni a carattere operativo, al cui interno, in seno al nucleo di gestione della crisi, siedono i referenti delle agenzie del comparto di sicurezza<sup>21</sup>.

in particolari ruoli e compiti in materia di difesa *cyber* tra i soggetti pubblici del sistema di informazione per la sicurezza della Repubblica.

<sup>1418</sup> V. le relazioni del DIS al Parlamento a partire dal 2017 e GORI (2014), pp. 5 – 29.

<sup>15</sup> V. Corte Cost., sentenza 24 maggio 1977, n. 86; v. per tutti VALENTINI (2008), p. 40 ss.; GIUPPONI (2010a), *Luigi Arcidiacono*, p. 1677 ss.; GIUPPONI (2010b), *Nuovi profili*, p. 53 ss.; CAIA (2022), p. 1037 ss.

<sup>16</sup> La sicurezza nazionale è il più recente approdo di un lungo cammino evolutivo politico, normativo e sociale, naturale riflesso della storia, piuttosto fibrillante, della Repubblica Italiana, che ha visto avvicinarsi diverse interpretazioni, figlie del loro tempo, su quali fossero i valori supremi da difendere: la ragion di Stato, la *salus rei publicae*, la sicurezza politica ed infine la sicurezza nazionale, ognuno di quali rappresenta, con sfumature diverse di significato, i valori supremi della Repubblica da proteggere. Per un approfondimento KOSTORIS (1964), p. 2 ss.; GREVI (1976 - 2012), p. 659 ss.; GREVI (1978), p. 230 ss.; PIZZETTI (1978), p. 81; MOSCA (1985), p. 190 ss.; BARILE (1987), p. 29; CONSO (1979), p. 179; PISA (1977), p. 1206; DI BITONTO (2006), p. 253. s.; MOSCA et al. (2008), *passim*; BONZANO (2010a), p. 5 ss.; GIUPPONI (2010a), p. 1677 ss.; GIUPPONI (2010b), p. 57 s.; BONZANO (2011); MORRONE (2010), p. 12; MOSCA (2012), p. 21; MAFFETTONE S. e MELIDORO D. (2015); GIUPPONI (2017), p. 856 ss.; MOSCA (2018), p. 5 s.; MOSCA (2018b); MOSCA (2019), p. 152; CALIGIURI (2021); GIUPPONI (2023), p. 1149 ss.; BIFULCO (2023), p. 1096 ss.; SALVI (2023), p. 248 ss.; Volendo anche RICOTTA (2023a).

<sup>17</sup> V. Corte Cost., sentenza 23 febbraio 2012, n. 40, v. PACE (2015), p. 1727.

<sup>18</sup> DE GENNARO (2019), p. 85.

<sup>19</sup> Per i riferimenti sull'attuale organizzazione del Sistema di Informazione per la Sicurezza della Repubblica (SISR) v. MOSCA et al (2008), MONTAGNESE A. e NERI C. (2016), p. 5 ss.; CAIA G. e BRESCIANI P. (2021), p. 329 ss.; CAIA (2022), p. 1037 ss.

<sup>20</sup> L'art. 5, c. 6, del d.l. n. 82/2021 precisa che il Copasir, ai sensi dell'art. 31, comma 3, della legge 3 agosto 2007, n. 124 “può chiedere l'audizione del direttore generale dell'Agenzia su questioni di propria competenza (art. 5, co. 6).

<sup>21</sup> Art. 8 del decreto-legge n. 82/2021.

La contiguità tra i sistemi è quindi evidente per struttura e per ragion d'essere, ma, come si vedrà nel paragrafo che segue, il legislatore non ha inteso qualificare l'Agenzia come di informazione per la sicurezza per ragioni che attengono alle mansioni istituzionali che è chiamata a svolgere, richiamando di conseguenza funzioni diverse (quindi non raccolta informativa a spettro variabile per scopi di sicurezza) e soprattutto un sistema di regole ordinarie e non speciali che diversamente contraddistinguono l'attività dei servizi di informazione per la sicurezza.

Cionondimeno, la convergenza del sistema cyber verso il Presidente del Consiglio e sotto l'usbergo delle responsabilità e dei poteri di alta direzione in materia di politiche di sicurezza dello Stato ha certamente una rilevanza perché, in ipotesi di rischio alla sicurezza nazionale, gli interessi, le libertà (*i.e.* economiche) o i poteri concorrenti (*i.e.* giudiziari) sono destinati ad essere soddisfatti in via recessiva, o addirittura a soccombere rispetto all'esercizio dei poteri politici presidenziali.

## 4. L'Agenzia per la cybersicurezza nazionale: un'agenzia di intelligence oppure no?

L'art. 5 del D.L. n. 82/2021 ha istituito l'Agenzia per cybersicurezza nazionale a tutela degli interessi nazionali nel capo della cybersicurezza. L'ACN è l'Autorità nazionale per la cybersicurezza, con personalità giuridica di diritto pubblico, dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria, guidata da un direttore generale<sup>22</sup>, che è l'organo di gestione nominato dal Presidente del Consiglio e al quale riferisce unitamente all'Autorità delegata, e consta di un vicedirettore e di un collegio dei revisori dei conti.

L'ACN è investita dalla legge del ruolo di nodo centrale per la cybersicurezza, l'unica Autorità nazionale per la difesa e la resilienza cibernetica<sup>23</sup>, competente per tutto un ampio spettro di attività a carattere regolamentare e investigativo: per la promozione e lo sviluppo di competenze e capacità tecnologiche, essa assume le iniziative idonee alla valorizzazione della crittografia e alla qualificazione dei servizi *cloud*, all'effettiva capacità di prevenire, rilevare e fornire risposte a incidenti e attacchi informatici, allo sviluppo di competenze e capacità industriali, tecnologiche e scientifiche e al raccordo tra le diverse amministrazioni dello Stato con competenze in materia di cybersicurezza.

Nel definire gli scopi istituzionali dell'ACN, dall'originario testo dell'art. 5 del decreto-legge n. 82/2021, è stato espunto in sede di conversione il riferimento alla tutela della sicurezza nazionale nello spazio cibernetico<sup>24</sup>. Come anticipato, la volontà legislativa, quindi, pare essere quella di collocare l'ACN al di fuori del comparto informativo di sicurezza, per ragioni che si radicano in esigenze di carattere operativo: *in parte qua* il DIS ha transitoriamente svolto un doppio ruolo di supplenza in materia di difesa e prevenzione dei rischi informatici, essendosi occupato dell'approvvigionamento informativo e della risposta in caso di minacce o incidenti alle infrastrutture critiche della nazione, svolgendo al contempo funzioni ispettive nei confronti degli enti vigilati all'interno perimetro di sicurezza e di coordinamento dell'attività dei ministeri coinvolti<sup>25</sup>.

Risulta evidente che il complesso delle mansioni attribuite oggi all'Agenzia cyber sia esorbitante rispetto alle funzioni istituzionali tradizionalmente affidate al comparto informativo per la sicurezza<sup>26</sup>: se diversamente fosse, si rischierebbe di gravare sulle capacità operative del

<sup>22</sup> Nominato tra i soggetti che possono essere nominati segretario generale della Presidenza del Consiglio, vale a dire magistrati delle giurisdizioni superiori, professori universitari di ruolo, dirigenti generali dello Stato, avvocati dello Stato o estranei alla pubblica amministrazione, purché in possesso di documentata esperienza nella gestione dei processi di innovazione. L'incarico dura 4 anni ed è rinnovabile una sola volta per non più di altri 4 anni.

<sup>23</sup> L'istituzione dell'Agenzia cyber ha consentito di risolvere la frammentazione delle competenze tra autorità diverse (Ministero dello sviluppo economico, Presidenza del Consiglio, DIS e Agenzia per l'Italia digitale).

<sup>24</sup> L'originario testo dell'art. 5 del decreto-legge 14 giugno 2021, n. 82, recitava “E' istituita, a tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico, l'Agenzia per la cybersicurezza nazionale”.

<sup>25</sup> Un ruolo assai determinante, tanto è vero che al fine di assicurare la prima operatività dell'Agenzia cyber è stato previsto che il personale del DIS addetto alla sicurezza cibernetica venga messo a disposizione dell'Agenzia ed impiegato nelle attività oggetto di trasferimento. V. Art. 17 del decreto-legge 14 giugno 2021, n. 82. V. anche SALVI (2022), p. 10.

<sup>26</sup> L'eccentricità delle funzioni dell'ACN rispetto a quelle di informazione per la sicurezza in senso stretto si può ricavare dalla sistematica: con la riforma attuata con la l. n. 124/2007, istitutiva dell'attuale Sistema di informazione per la sicurezza della Repubblica (SISR), il legislatore

sistema, motivo per il quale è stato necessario affidare a una agenzia *ad hoc* compiti che idealmente coprono tutto lo spettro delle attività necessarie a garantire una tutela ottimale nel dominio *cyber*.

Da una diversa prospettiva, le ragioni di una differenziazione circa la natura dell’Agenzia è essenziale sul piano delle attività che è chiamata a condurre. Gli organismi di informazione per la sicurezza agiscono secondo un modello unico nel suo genere, che coniuga una tendenziale libertà delle forme nei modi della raccolta informativa e nell’attività operativa con la pressoché totale segretezza dell’intero comparto circa l’attività, i mezzi, le strutture, il personale, le finanze, regole e protocolli interni. Modello, quest’ultimo, che difficilmente potrebbe contraddistinguere l’Agenzia Cyber, la cui attività ha invece una spiccata proiezione esterna.

Così, inaugurando l’ACN, si è costituito un unico ente regolatore di diritto pubblico che, poiché collocato al di fuori del sistema di informazione per la sicurezza della Repubblica, garantisce maggiore trasparenza, efficacia e garanzia nei rapporti tra enti pubblici e con i soggetti privati, soprattutto in sede di esercizio dei poteri ispettivi e di vigilanza.

Quindi, se da un lato gli interessi in materia cibernetica rientrano nello spettro delle attribuzioni in materia di sicurezza nazionale che fanno capo al Presidente del Consiglio dei ministri, dall’altro, il legislatore non ha inteso qualificare l’agenzia come un organismo di informazione per la sicurezza, e quindi non le ha attribuito tutta una serie di prerogative speciali e derogatorie che diversamente caratterizzano l’attività di quest’ultimo comparto<sup>27</sup>. Da qui, se ne possono trarre alcune conseguenze: l’Agenzia agisce su mandato del Presidente del Consiglio ma secondo il paradigma procedimentale ordinario, dovendosi escludere l’applicazione della speciale normativa prevista dalla legge n. 124/2007 al di fuori di quelle disposizioni, come in materia di poteri presidenziali e segreto di Stato, che hanno portata generale.

## 5. **Segue. L’inapplicabilità della speciale disciplina in materia di attività di informazione per la sicurezza della Repubblica.**

Una delle conseguenze dell’esclusione dell’Agenzia *cyber* dal novero degli organismi che compongono il Sistema di informazione per la sicurezza è la sostanziale inapplicabilità della speciale disciplina prevista dalla legge n. 124/2007, oltreché delle numerose disposizioni del codice di procedura penale poste a tutela delle speciali funzioni del comparto informativo per la sicurezza<sup>28</sup>.

Una prima, sostanziale, differenza si riscontra sul piano della segretezza. Pressoché ogni aspetto dell’attività, delle scelte e dell’organizzazione degli organismi di informazione per la sicurezza è coperto, o è assoggettabile, al segreto di Stato<sup>29</sup>. Diversamente, l’Agenzia non è vincolata allo stesso regime di segretezza in ragione delle funzioni che la legge le attribuisce, in particolare quelle di vigilanza ed ispezione, che per essere esercitate richiedono lo svolgimento di attività palesi ed una certa *discovery* informativa.

---

ha inteso conferire piena autonomia alle funzioni dei Servizi, separando in via ordinaria l’attività di informazione per la sicurezza da quella preventiva e repressiva tipica delle forze di polizia (vista l’evidente contiguità tra quest’ultime funzioni, la separazione limita potenziali sovrapposizioni v. (GAMBACURTA (2008B), p. 304 ss.; GIUPPONI (2009), p. 2 s.; CAIA (2022), p. 1045). La peculiare natura della funzione amministrativa specializzata dell’informazione per la sicurezza (v. CAIA (2022), p. 1037 ss.), risulta determinante poiché si riverbera anche sul piano delle finalità rispetto alle quali anche le attività operative possono essere compiute: i Servizi operano esclusivamente sul piano della raccolta informativa per finalità di tutela della sicurezza nazionale, che è attività più ampia della funzione preventiva e svolta dalle forze di polizia (v. JEMOLO (1995)) Per contro, l’autorità di pubblica sicurezza ha un ambito di competenza generalizzata in materia di prevenzione e repressione: è quindi questa l’autorità preposta in via ordinaria a ricorrere a misure attive, a carattere operativo, adottate in funzione di tutela fattiva della sicurezza pubblica. La legge n. 801/1977 aveva istituito appositi Servizi per le *informazioni e la sicurezza*, mentre l’assetto oggi definito dalla l. n. 124/2007 richiama per i Servizi l’attività di *informazione per la sicurezza*. La differenza tra queste due diverse formulazioni non è meramente lessicale: con servizi di *informazione e sicurezza* si intendeva richiamare l’attribuzione ai Servizi di poteri per il compimento di azioni operative dirette a tutelare la sicurezza interna; viceversa, con attività di *informazione per la sicurezza* la riforma ha inteso ribadire la centralità dei compiti informativi (v. in particolare GIUPPONI (2009), p. 2 s), separandoli da quelli di sicurezza in senso stretto che spettano in via principale alle autorità di pubblica sicurezza.

<sup>27</sup> Si tratta di una soluzione in linea con le funzioni attribuite all’Agenzia, tant’è che i provvedimenti adottati dall’Agenzia *cyber* sono sindacabili innanzi al Giudice Amministrativo, vista l’aggiunta all’art. 135 del codice del processo amministrativo, in materia di competenza funzionale inderogabile del Tar Lazio, sede di Roma, a giudicare “le controversie aventi ad oggetto i provvedimenti dell’agenzia per la cybersicurezza nazionale”.

<sup>28</sup> *Infra* in questo §.

<sup>29</sup> Sono suscettibili di apposizione del segreto di Stato pressoché tutte le informazioni sull’attività e l’organizzazione degli organismi di informazione per la sicurezza V. in particolare l’art. 5 del D.P.C.M. dell’8 aprile 2008.

Resta comunque invariato il potere-dovere di proteggere tutte quelle informazioni sensibili che si generano nel corso dell'attività istituzionale, secondo le regole ordinarie previste dalla legge n. 124/2007: ogni qual volta si origini un'informazione che non deve essere divulgata per ragioni di sicurezza<sup>30</sup>, il personale si adopera per garantirne la riservatezza ed informare il Presidente del Consiglio e l'Organizzazione Nazionale per la sicurezza affinché sia apposto il segreto di Stato o una classifica di segretezza. Questo vale anche nei rapporti con l'accertamento condotto in parallelo dall'autorità giudiziaria, alla quale il segreto di Stato può essere opposto secondo le regole di applicazione generale previste dal codice di procedura penale e dalla legge n. 124/2007<sup>31</sup>.

Discorso diametralmente opposto deve essere fatto per la comunicazione della notizia di reato, ex art. 23 della l. n. 124/2007, e per l'applicazione delle speciali garanzie funzionali contenute all'art. 17 della legge n. 124/2007<sup>32</sup> e agli artt. 256 *bis*<sup>33</sup> e 270 *bis*<sup>34</sup> c.p.p.: si tratta di disposizioni eccezionali che, come tali, non possono essere applicate in via estensiva.

## 6.

### Segue. La comunicazione della notizia di reato.

La questione delle esigenze connesse alla tutela della sicurezza nazionale assume particolare rilievo in relazione dell'obbligo di denunciare la notizia di reato prescritto all'art. 331 c.p.p. per tutti i pubblici ufficiali e gli incaricati di pubblico servizio che, nell'esercizio delle loro funzioni, abbiano conoscenza di un reato perseguibile di ufficio.

Nel sistema di informazione per la sicurezza, ragioni di stretta necessità correlate al perseguimento delle relative funzioni istituzionali consentono ai direttori delle agenzie che compongono il Sistema di ritardare la comunicazione della notizia di reato (art. 23 l. n. 124/2007).

Poiché il potere di ritardare la comunicazione della *notitia criminis* risulta essenzialmente legato a ragioni di sicurezza nazionale, potrebbe accadere che anche nel sistema cyber sorga la necessità di non comunicare tempestivamente la notizia di reato per non compromettere l'azione dell'Agenzia o aggravare la crisi: c'è allora da domandarsi se per l'ACN questo sia possibile in assenza di una specifica disposizione di legge.

Nell'attività di informazione per la sicurezza, ai sensi dell'art. 23 l. n. 124/2007<sup>35</sup> il personale del contingente speciale ex art. 21 della l. n. 124/2007 non riveste la qualifica, salvo il caso di concessione temporanea, né di agente/ufficiale di pubblica sicurezza né di polizia giudiziaria, risultando di conseguenza sgravato da tutta una serie di adempimenti e obblighi

<sup>30</sup> Vige in materia di segreto di Stato una regola generale, cardine del sistema: pubblici ufficiali, incaricati di pubblico servizio o impiegati pubblici hanno l'obbligo di non divulgare e di mantenere il riserbo sulle notizie coperte da segreto di Stato, sancito in via generale all'art. 41 legge n. 124/2007 rubricato "Divieto di riferire riguardo a fatti coperti dal segreto di Stato.

<sup>31</sup> In particolare, alle disposizioni in materia di tutela del segreto di Stato nel corso dell'attività acquisitiva degli elementi di prova dichiarativa (art. 202 c.p.p.) o documentale (artt. 256 s. c.p.p.). In via generale, il segreto di Stato viene sempre tutelato, a prescindere da dove si generi la notizia riservata o da chi ne sia in possesso: sicché, ogni qual volta la legge tutela la segretezza dell'informazione, dovrà applicarsi la relativa disciplina. Con particolare riferimento all'accertamento penale, il dovere di tutelare il segreto di Stato si declina in tutti i principali momenti dell'acquisizione probatoria, prescrivendo specifiche regole che hanno la funzione di non compromettere né il segreto né tantomeno le attribuzioni del Governo. Quando il segreto è opposto, l'autorità giudiziaria interpella il Presidente del Consiglio affinché confermi o meno il segreto di Stato, e nelle more della decisione ha il dovere di astenersi da qualsiasi condotta volta all'acquisizione della notizia per la quale è stato opposto il segreto. v. BONZANO (2008), p. 24 ss.; BONZANO (2011), p. 586 ss.; v. anche SPANGHER (1993), p. 471 ss.; CERRUTI (2013), p. 35 s.; DELL'ANNO (2020), p. 220; BONZANO (2023), p. 3649 ss.; volendo anche RICOTTA (2023b).

<sup>32</sup> L'art. 17 della l. n. 124/2007 prevede che gli appartenenti agli organismi di informazione non siano punibili qualora ricorrano ad azioni punite come reato ma indispensabili per le finalità di sicurezza, purché autorizzati e non si tratti di condotte espressamente escluse dalla speciale causa di giustificazione (artt. 17 e 18 l. n. 124/2007) v. MOSCA (2008), p. 235 ss.; MOSCA (2018a), p. 115 ss.; CAIA (2022), p. 1047 s.

<sup>33</sup> L'art. 256-*bis* c.p.p. prescrive una speciale procedura di acquisizione documentale custodita presso le sedi delle agenzie che afferiscono al sistema di informazione per la sicurezza della Repubblica e che sia sottoposta a segreto di Stato: il pubblico ministero non può procedere coattivamente né alla perquisizione né al sequestro, ma deve trasmettere necessariamente un previo ordine di esibizione avendo cura di specificare gli incartamenti di interesse investigativo e i motivi per cui sta procedendo. L'ordine di esibizione instaura una procedura controllata di divulgazione: se non è apposto il segreto di Stato e i documenti esistono, il pubblico ministero può esaminare la documentazione in sede con la collaborazione del personale dell'agenzia. Questo significa che, impregiudicato il segreto di Stato, il divieto di attività coercitive di perquisizione e sequestro di iniziativa dell'organo dell'accusa nei confronti dell'Agenzia non dovrebbe essere *tout court* applicabile, se non limitatamente ai luoghi e alle funzioni che vedono la diretta partecipazione dei Servizi, come nel nucleo per la cybersicurezza e gestione della crisi v. DELL'ANNO (2022), p. 224 s.; RIVELLO (2023a), p. 3381 - 3383.; RIVELLO (2023b), p. 3383 - 3385.

<sup>34</sup> Non può ritenersi applicabile la specifica disciplina dell'art. 270-*bis* c.p.p. sulla inutilizzabilità delle intercettazioni qualora siano state captate comunicazioni di servizio tra appartenenti al Sistema di informazione per la sicurezza. La norma accorda infatti la garanzia della regola di esclusione probatoria seguendo un criterio funzionale e soggettivo: soltanto le conversazioni di servizio che non abbiano natura squisitamente privata, purché provengano da interlocutori che appartengono al sistema di informazione per la sicurezza. BONZANO (2023), p. 3649 ss.; DELL'ANNO (2020), p. 228 s.

<sup>35</sup> V. GAMBACURTA (2008a), p. 287 ss.

tipici di quest’ultime funzioni (e.g. il dovere di intervento e di arresto obbligatorio in flagranza) nonché, con particolare riferimento alla P.G., dalla subordinazione al pubblico ministero.

L’esclusione di quest’ultime qualifiche non significa che il personale non sia da considerarsi, comunque, un pubblico ufficiale (alla stregua dei criteri dell’art. 357 c.p.p.): per questo, l’art. 23 l. n. 124/2007 non elimina *tout court* l’obbligo di denuncia dei fatti che costituiscono reato, ma stabilisce, in deroga al regime ordinario, una procedura *ad hoc*: se nell’ambito dell’attività informativa emergono fatti che costituiscono un reato, in un primo passaggio interno il personale comunica l’esistenza del reato ai direttori delle rispettive agenzie o al direttore generale del DIS, che a loro volta hanno l’obbligo di comunicarla alla polizia giudiziaria (e non direttamente al pubblico ministero), che a sua volta ne cura la successiva trasmissione all’ufficio di Procura. A differenza che nel regime ordinario, in questo caso la trasmissione della notizia e delle relative informazioni può essere intempestiva qualora sia strettamente necessario al perseguimento delle finalità istituzionali del Sistema di informazione: previa autorizzazione del Presidente del Consiglio, l’art. 23 della l. n. 124/2007 consente ai già citati direttori di ritardare la comunicazione della notizia di reato.

La *ratio* dell’art. 23 della l. n. 124/2007 è quella di garantire la reciproca autonomia ed equilibrare i rapporti tra potere esecutivo e giudiziario, aprendo al contempo un canale di comunicazione che serve ad acquisire elementi utili a fini investigativi salvaguardando le prerogative degli organismi di informazione<sup>36</sup>. L’evidente specialità della disciplina, legata all’esercizio delle funzioni di informazione per la sicurezza, a rigore di logica non ne consente l’estensione all’ACN, i cui funzionari, in assenza di una disposizione analoga all’art. 23 della l. n. 124/2007 ed in virtù della propria qualifica di pubblici ufficiali, sono tenuti a comunicare, sempre e senza ritardo, la notizia di reato al pubblico ministero o alla polizia giudiziaria.

Si potrebbe sostenere che, anche in assenza di una disciplina *ad hoc*, ragioni di sicurezza nazionale legate al dominio cibernetico consentirebbero al Presidente del Consiglio, nell’esercizio dei suoi poteri di Alta direzione, di intervenire per evitare o limitare la diffusione di una notizia avvalendosi dello strumento della segretezza, che avrebbe l’effetto, diretto o indiretto, di non portare a conoscenza dell’autorità giudiziaria fatti dai quali si potrebbe trarre l’esistenza di un reato.

Si tratta, tuttavia, di una questione particolarmente delicata, come tale refrattaria a soluzioni *tranchant*. Questo perché, nell’ottica della disciplina della l. n. 124/2007, l’esigenza di segretezza è insita nell’informazione o nella notizia della quale è pericolosa *ex se* la diffusione, a prescindere dal soggetto che la origina o che dovrebbe esserne il destinatario<sup>37</sup>: se ne ricorrono i presupposti, e ci si trova al di fuori delle ipotesi di segreto vietato<sup>38</sup>, pressoché tutto può essere sottoposto a segreto di Stato.

Al tempo stesso, il meccanismo dell’art. 23 della l. n. 124/2007 disciplina un procedimento evidentemente eccezionale, in deroga al dovere generale stabilito per i pubblici ufficiali e gli incaricati di pubblico servizio ex art. 331 c.p.p., che si muove sul terreno del delicato equilibrio tra poteri dello Stato e del necessario rispetto dell’autonomia e delle diverse attribuzioni del potere esecutivo e di quello giudiziario<sup>39</sup>: il solo fatto che la menzionata disposizione esista, in altre parole, avrebbe la conseguenza di non lasciare spazi a meccanismi di ritardata comunicazione della *notitia criminis* al di fuori di quelli già espressamente previsti dalla legge. Del resto, se il segreto è pur sempre la condizione naturale dell’attività investigativa, quello di Stato si contraddistingue per essere l’*extrema ratio* e non uno strumento ordinario di gestione della crisi.

## 7.

### I poteri investigativi dell’Agenzia per la cybersicurezza nazionale e le indagini dell’autorità giudiziaria.

Se da un lato la legge n. 124/2007 continua a costituire il paradigma normativo per il complesso delle attività legate alla politica informativa di sicurezza, dall’altro, il d. l. n. 82/2021

<sup>36</sup> Cfr. GAMBACURTA (2008a), p. 292.

<sup>37</sup> Per la cd. “concezione ontologica” del segreto di Stato cfr. Corte Cost., sentenza 3 aprile 2009, n. 106; v. BONZANO (2010b), p. 301 ss.; v. anche PACE (2015), p. 1719 ss.; in generale, sull’apposizione del segreto di Stato, v. SCANDONE (2008), p. 499 ss.; BONZANO (2008), p. 17 ss.; GIUPPONI (2010a), p. 1684 ss.; CAIA (2022), p. 1037 ss.; volendo, anche RICOTTA (2023a).

<sup>38</sup> Ex art. 39 c. 11 l. n. 124/2007 e art. 204 c.p.p.

<sup>39</sup> V. GAMBACURTA (2008a), pp. 291-292.

ha il pregio di cristallizzare un sistema di difesa e resilienza informatica *ad hoc*, chiamato ad operare, per ragioni di sistema, in sinergia con il comparto di informazione per la sicurezza e sotto l’egida del Presidente del Consiglio nel suo ruolo di organo di vertice delle politiche di sicurezza dello Stato, ma con competenze, mezzi e funzioni altamente specializzate in virtù del dominio operativo e delle specifiche attribuzioni dell’ACN.

La capacità di prevenire e rilevare attacchi e minacce alle infrastrutture digitali, così come quella di vigilare sugli enti allo scopo di monitorare la corretta attuazione e implementazione delle misure di natura tecnica e organizzativa, accertare le violazioni e irrogare eventuali sanzioni, l’art. 7 del d.l. n. 82/2021 attribuisce all’Agenzia un complesso di poteri autoritativi di natura amministrativa, funzionali alla sorveglianza, al controllo sul rispetto degli obblighi sugli enti inseriti nel perimetro di cyber-sicurezza o destinatari delle direttive NIS. A questi poteri, si sommano quelli previsti dall’art. 41 del Codice delle comunicazioni elettroniche, che ribadiscono il potere dell’Agenzia cyber di verificare l’adeguatezza organizzativa e indagare i casi di mancata conformità alle prescrizioni tecnico-organizzative ed i relativi effetti sulla sicurezza delle reti e dei servizi.

Questa funzione di vigilanza si esplica necessariamente attraverso l’esercizio di tutta una serie di poteri a carattere ispettivo/investigativo, come il potere di richiedere l’esibizione o la trasmissione di dati, notizie e documenti, invitare il soggetto vigilato a comparire per fornire indicazioni o procedere all’esecuzione di accessi, ispezioni e verifiche<sup>40</sup>.

Poteri che l’agenzia esercita in proprio, ma anche avvalendosi della collaborazione delle Forze di Polizia, anche alla luce dello stretto coordinamento con il nucleo di Polizia di Stato e delle telecomunicazioni e del CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche)<sup>41</sup>.

Poiché ogni possibile attacco informatico può costituire anche un crimine penalmente sanzionato<sup>42</sup>, è altamente probabile che l’investigazione dell’Agenzia *cyber* si intersechi con quella dell’Autorità giudiziaria: una volta che è emersa la notizia di reato, a rigore di logica i pubblici ufficiali dell’ACN dovrebbero tempestivamente comunicarla all’autorità giudiziaria, il pubblico ministero iscriverla nel relativo registro, anche nel caso in cui sia ignoto l’autore del reato, e conseguentemente avviare formalmente le indagini preliminari.

Rilevano allora due profili di interesse: le garanzie applicabili all’investigazione amministrativa una volta che sia emersa una notizia di reato; la possibile sovrapposizione tra ACN e Procura della Repubblica, alla luce del fatto che entrambe hanno competenze e responsabilità in materia di investigazioni ma manca, nel decreto, una norma che le coordini.

## 8.

### Cenni sulla migrazione dei risultati dell’inchiesta amministrativa e sull’art. 220 disp. att. c.p.p.

Il passaggio dall’attività di investigazione amministrativa all’indagine preliminare del pubblico ministero è regolato in via generale dall’art. 220 disp. att. c.p.p.<sup>43</sup>, a norma del quale “quando nel corso di attività ispettive o di vigilanza previste da leggi o decreti emergono indizi di reato, gli atti necessari per assicurare le fonti di prova e raccogliere quant’altro possa servire per l’applicazione della legge penale sono compiuti con l’osservanza delle disposizioni

<sup>40</sup> Così l’art. 13 della legge 24 novembre 1981 n. 689. Si v. SORBELLO (2016), p. 128; v. anche FURGUELE (2020), p. 147 ss.

<sup>41</sup> L’art. 7 d.l. n.82/2021 specifica ulteriormente che le funzioni dell’agenzia sono esercitate nel rispetto delle attribuzioni delle altre amministrazioni dello Stato, e in particolare del Ministro dell’interno che è l’autorità nazionale di pubblica sicurezza. In questo caso il riferimento al Ministro dell’Interno valorizza la funzione principale del dicastero, e cioè quella di garantire l’ordine e la sicurezza pubblica, dalla quale scaturiscono competenze specifiche in termini sia di polizia giudiziaria che di polizia di sicurezza. Peraltro, è proprio all’interno di tale Ministero che opera il principale raccordo operativo dell’ACN con le forze di polizia in caso di minacce, attacchi e criminalità informatica, vale a dire il Centro Nazionale Anticrimine. Peraltro, è proprio all’interno di tale Ministero che opera il principale raccordo operativo dell’ACN con le forze di polizia in caso di minacce, attacchi e criminalità informatica, vale a dire il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (il CNAIPIC), l’organo istituito allo scopo di garantire la sicurezza e la regolarità dei servizi di telecomunicazione e delle infrastrutture critiche di interesse nazionale dall’art. 7-bis, c. 1 del DPR n. 144/2005.

<sup>42</sup> Del resto, l’adesione alla convenzione di Budapest ha consentito l’introduzione, a livello dell’Unione Europea, di un modello normativo comune per il contrasto alla criminalità informatica, che ha di fatto consentito di criminalizzare qualsiasi condotta che costituisca un attacco informatico a una infrastruttura critica v. CADOPPI *et al.* (2019).

<sup>43</sup> Si v. NOBILI (1984), p. 376 s.; KOSTORIS (1990), p. 73 s.; ORLANDI (1992), p. 93; FUMU (1992), p. 100 s.; CESARI (1993), p. 214 s.; SCALFATI (2020), p. 1 ss.; FURGUELE (2020), p. 141 s.; GALANTINI (2022), p. 999 ss.; GALLUCCIO MEZIO (2023a), p. 3712 s.

del codice<sup>44</sup>.

La norma non codifica un vero e proprio passaggio di consegne tra indagine amministrativa e penale, poiché nel rispetto delle reciproche attribuzioni i due procedimenti possono proseguire in parallelo<sup>45</sup>, ma segna un momento, l'emersione della notizia di reato, a partire dal quale risulta necessario che gli elementi investigativi vengano raccolti con l'osservanza delle regole del rito, per non frustrare o aggirare le relative garanzie<sup>46</sup>.

L'art. 220 disp. att. c.p.p. costituisce una regola di legittimità dell'acquisizione delle fonti di prova<sup>47</sup> e ne condiziona la futura utilizzabilità nel processo penale se, nel corso dell'attività amministrativa, non sono state rispettate le garanzie prescritte dalla legge.

Il richiamo dell'art. 220 disp. att. c.p.p. alle attività ispettive e di vigilanza non deve essere interpretato in senso restrittivo ma estensivo, poiché non si limita a richiamare due particolari tipi di accertamento ma il generale esercizio di poteri istruttori di natura amministrativa, nell'ambito del quale emerga la conoscenza di un fatto che abbia rilevanza penale<sup>48</sup>.

La conseguenza della violazione dipende dalle regole che sono previste garanzie che la legge prescrive per ciascun atto investigativo, come la facoltà di nominare e farsi assistere da un difensore nel momento in cui si rendono dichiarazioni<sup>49</sup> (ex artt. 63 e 350 c.p.p.) o nel corso di una perquisizione o di un accertamento tecnico irripetibile<sup>50</sup>, secondo la disciplina del codice a cui l'art. 220 disp. att. c.p.p. rimanda<sup>51</sup>.

La regola aurea è che quanto più si applicano garanzie difensive alle attività extra-procedimentali, tanto più si garantisce il *continuum* tra procedura amministrativa e investigazione penale. Così per l'acquisizione degli elementi di prova valgono certamente le regole di procedura penale ai fini dell'utilizzabilità e le garanzie procedurali per i mezzi di ricerca della prova e, soprattutto, per gli accertamenti investigativi, con particolare riferimento a quelli che comportino una modificazione irreversibile dell'oggetto di prova.

Nella prospettiva di un possibile futuro dibattito, sarà necessario garantire, chiunque sia l'autorità che materialmente conduce in quel momento le indagini e procede ai necessari accertamenti di natura tecnica, la partecipazione dell'interessato laddove sia possibile ed il rispetto dei protocolli forensi per assicurare affidabilità e controllabilità dell'elemento di prova raccolto. L'Agenzia *cyber* è del resto pensata per svolgere accertamenti ad alto livello di professionalità tecnica, che può corroborare ricorrendo anche ad enti terzi, pubblici o privati, dotati

<sup>44</sup> Alla disposizione richiamata fa da naturale *pendant* l'art. 223 disp. att. in materia di analisi e campionamenti non rivedibili, per le quali sono prescritte garanzie difensive e partecipative dell'interessato. L'art. 223 disp. att. è infatti legato all'art. 220 disp. att. da un rapporto di *genus ad speciem*, prescrivendo una particolare procedura garantita da applicare laddove, nel corso delle attività di ispezione e vigilanza contemplate all'art. 220 disp. att., si renda necessario procedere per la prima volta ad esami o a analisi non ripetibili, oppure, laddove sia materialmente possibile, l'interessato domandi all'autorità amministrativa la revisione delle analisi già effettuate cfr. GALLUCCIO MEZIO (2023b), p. 3725 ss.

<sup>45</sup> KOSTORIS (1990), p. 81; MAZZA (2000), p. 1280 s.; BONTEMPELLI (2009), p. 130 s.; RAMPIONI (2019), p. 241.

<sup>46</sup> NOBILI (1984), p. 376; UBERTIS (1992), p. 431; FURGIUELE (2020), p. 145.

<sup>47</sup> Cass., Sez. III, 18 novembre 2014, n. 4919; Cass., Sez. III, 10 febbraio 2010, in *C.E.D. Cass.* n. 246599; Cass., Sez. V, 23 settembre 2004, n. 43542, in *questa rivista*, 2006, p. 2542.; *contra* si v. FURGIUELE (2020), p. 159. Inoltre, l'osservanza di tale previsione rileva anche ai fini della eventuale illiceità disciplinare o addirittura penale derivante da quanto accaduto nel corso dell'attività ispettiva o di vigilanza.

<sup>48</sup> Il collegamento tra le due inchieste si fonda quindi sull'emersione di indizi di reato, vale a dire nella possibilità di "attribuire rilevanza penale al fatto che emerge dall'inchiesta amministrativa e nel momento in cui emerge, a prescindere dalla circostanza che esso possa essere riferito ad una persona determinata" (cit. Cass., Sez. Un., 28 novembre 2001, n. 45477, in *Giur. it.*, 2002, pag. 1235), vale a dire che siano emersi tutti gli elementi costitutivi (Cass., Sez. III, 4 giugno 2019, n. 31223, in *C.E.D. Cass.* n. 276679): una volta emersi gli indizi, si deve ritenere che sia stata avviata sostanzialmente una indagine penale, a prescindere che sia già stata formulata e iscritta la notizia di reato nel registro del pubblico ministero o siano già state individuate le norme di legge che si assumono violate (Cass., Sez. III, 24 settembre 2001, in *Giur. it.*, 2002, pag. 1035; v. CESARI (1993), p. 215; MAZZA (2000), p. 1280 s.; SORBELLO (2016), p. 134.). La semantica dell'art. 220 disp. att. mira evidentemente ad escludere la regola nelle ipotesi in cui vi sia soltanto un mero sospetto, e quindi dell'emersione di una situazione di fatto che si contraddistingue per una capacità argomentativa e dimostrativa minore, perché l'ipotesi del fatto si basa soltanto su intuizioni soggettive o è priva di riscontri oggettivi o, qualora presenti, anche questi siano insufficienti. Sulla differenza tra indizio e sospetto si veda UBERTIS (1995), p. 296 s; con specifico riferimento al fatto che l'utilizzo del termine emersione indicherebbe nell'art. 220 disp. att. c.p.p. uno stato embrionale dell'indizio di reato v. FURIN (1999), p. 2722 s. È discusso invece se "indizi di reato" sia una formula equivalente a "notizia di reato", v. KOSTORIS (1990), p. 83; ORLANDI (1992), p. 156; oppure no v. APRATI (2010), p. 17 s. Va da sé che il fatto di reato così qualificato impone la sua comunicazione al pubblico ministero ai sensi dell'art. 347 c.p.p. (PAULESU (2023), p. 1509 ss.): *in parte qua*, seguendo le regole generali, gli operatori dell'Agenzia, a cui la legge attribuisce espressamente la qualifica di pubblico ufficiale nell'esercizio delle loro funzioni di ispezione e vigilanza, sono da considerare come ufficiali di polizia giudiziaria quantomeno ai fini dell'acquisizione della notizia di reato.

<sup>49</sup> Sul diritto al silenzio nei procedimenti amministrativi si v. CANESCHI (2020), p. 579 ss.; SFORZA (2022), p. 83 s.; BONZANO (2023), p. 47 s.

<sup>50</sup> L'art. 223 disp. att. prevede che qualora nel corso di attività ispettive o di vigilanza si devono eseguire analisi per le quali non è prevista la revisione, deve essere dato avviso all'interessato del luogo e dell'ora dove le analisi avranno luogo, affinché possa presenziare o farsi assistere da una persona di fiducia. In questo caso, se l'accertamento non rivedibile, vale a dire laddove l'oggetto dell'analisi sia soggetto a modificazione irreversibile, consentiva di integrare soggettivamente l'assunzione della prova con la presenza dell'interessato, che in presenza di indizi di reato doveva già qualificarsi come sottoposto ad indagine, si cristallizzerà l'inutilizzabilità nel momento in cui si sia proceduto in difetto dell'avviso ex art. 360 c.p.p.

<sup>51</sup> FURGIUELE (2020), p. 160.

di comprovate capacità operative. Lo spirito della normativa vuole incentivare la cooperazione delle società in funzione di evolvere le competenze di azione e prevenzione, a beneficio del sistema. Va da sé che, come già accade quando nell'inchiesta penale il pubblico ministero si avvale di privati nello svolgimento di attività che richiedono competenze particolari, essi agiscono sotto la direzione e la responsabilità del soggetto pubblico<sup>52</sup>.

## 9. La concorrenza investigativa.

È già stato anticipato come lo spirito della normativa sia quello di incentivare la cooperazione tra diverse autorità. Le competenze sono ripartite su quattro pilastri, *cyber-defence*, *cyber-intelligence*, *cyber-resilienza* e *cyber-investigation*, attribuite a istituzioni differenti secondo un criterio di specializzazione delle funzioni: il ministero della difesa si occupa della difesa in senso stretto nel dominio *cyber*; il comparto di informazione per la sicurezza raccoglie e analizza le notizie, elabora e dissemina le informazioni, e si adopera per le azioni operative più opportune; l'Agenzia *cyber* investiga e adotta provvedimenti di ripristino e futura risposta; i reparti di polizia specializzata procedono alle indagini di polizia giudiziaria sotto la direzione dell'autorità giudiziaria, che esercita l'azione penale se ravvisa ipotesi di reato.

È dunque possibile che l'intervento congiunto dell'Agenzia e della Procura possa generare attriti, alla luce del fatto che entrambe, nonché le diverse forze di polizia che ne coadiuvano l'attività, hanno certamente competenze e responsabilità in materia di investigazioni, ma non c'è perfetta sovrapposibilità o concomitanza di interessi.

L'Agenzia è pensata per un intervento di immediata prossimità. Verosimilmente, essendo il punto di contatto che per primo riceve la notifica dell'incidente, è la prima autorità che interviene, e deve giungere sulla scena non appena la crisi si manifesta o l'incidente accade con il compito di ricostruire tempestivamente le cause dell'accadimento prima che i dati o gli elementi utili si disperdano o vengano irrimediabilmente compromessi, e soprattutto ripristinare il sistema, evitare ulteriori pregiudizi, attuali e futuri, alla sicurezza delle reti e dei sistemi. L'Agenzia assolve quindi ad una triplice funzione ripristinatoria, investigativa e di creazione di futura sicurezza.

La Procura invece nutre un interesse meno tecnico, non di sicurezza in senso stretto, che è la proiezione dei propri doveri istituzionali di acquisire e assicurare le fonti di prova in funzione dell'accertamento, quindi nell'ottica di costituirsi elementi spendibili nel procedimento e nel processo penale.

Un esempio, seppur potenzialmente virtuale<sup>53</sup>, di conflitto tra autorità potrebbe accadere se si verificasse una stasi dell'attività di indagine *cyber* provocata dall'esecuzione di un provvedimento di sequestro di dispositivi, dei sistemi o di parte degli impianti coinvolti nell'inchiesta. Una stasi che non gioverebbe all'Agenzia, perché la sua funzione non è soltanto accertare le cause della crisi, ma anche evitare il propagarsi di ulteriori pregiudizi all'integrità e alla sicurezza: per ragioni di necessità l'Agenzia potrebbe intervenire per ripristinare lo *status quo ante* evitando ulteriori compromissioni della sicurezza e coinvolgendo soltanto successivamente l'ufficio di Procura. Questo vale anche se l'intervento tempestivo dell'Agenzia sacrifica elementi utili per le indagini penali o se la situazione non consente il rispetto delle garanzie del rito (e quindi, beninteso, la spendibilità probatoria degli elementi raccolti in difformità dal codice di rito).

A differenza che in altre investigazioni di sicurezza<sup>54</sup>, come quelle in ipotesi di disastro

<sup>52</sup> Per i profili circa la commistione investigativa tra pubblico e privato nel processo penale si rimanda a CESARI (2021), p. 1174 s.

<sup>53</sup> Seppur, si deve osservare, che la stessa natura critica delle infrastrutture difficilmente farebbe sorgere la necessità, da parte del pubblico ministero, di sequestrare l'intero impianto o adottare un provvedimento che provochi la sostanziale stasi dell'infrastruttura, con gravi ripercussioni sulle relative funzioni cruciali.

<sup>54</sup> Una situazione di concorrenza investigativa fra autorità amministrativa e giudiziaria, molto vicina a quella appena descritta, ricorre in caso di disastro aereo che riporti delle vittime tra personale di bordo o passeggeri. Sorgono in questo caso diverse necessità: comprendere le cause dell'evento ed evitare che si replichino nel tempo, attraverso attività d'indagine ultra-specializzate al fine di assicurare le fonti di prova e risultati quanto più attendibili possibile, che prende il nome di "inchiesta di sicurezza", che l'art. 2 del regolamento UE n. 996/2010 definisce come "un insieme di operazioni svolte da un'autorità investigativa per la sicurezza ai fini della prevenzione degli incidenti ed inconvenienti, che comprende la raccolta e l'analisi di dati, l'elaborazione di conclusioni, la determinazione della causa o delle cause e/o di fattori concorrenti e, ove opportuno, la formulazione di raccomandazioni in materia di sicurezza". Al riguardo, è stata istituita in Italia, con il d.lgs. n. 66/1999 (come modificato dal dpr. n. 189/2010 e dal regolamento UE n. 996/2010), una agenzia *ad hoc* che opera in condizioni di terzietà, l'Agenzia nazionale per la sicurezza del volo (ANSV) con poteri investigativi e sanzionatori; per un approfondimento v. FRANCHI (2015), pp. 3 ss.;

aereo, nell'architettura cyber non c'è un meccanismo che regoli l'indagine amministrativa con quella penale, disciplinando il coordinamento dei rispettivi atti istruttori o prevedendo regole che attribuiscono espressa preferenza all'una o all'altra inchiesta, evitando sovrapposizioni o conflitti.

In assenza di meccanismi formali<sup>55</sup>, in questo specifico contesto il rango della sicurezza cibernetica, nel prisma della sicurezza nazionale, costituisce una direttrice di coordinamento: quando esigenze di sicurezza nazionale lo rendono necessario, le prerogative connesse ai poteri di alta direzione delle politiche di sicurezza, legittimano l'Agenzia ad un pieno intervento, che può svolgersi, ove necessario, *inaudita altera parte*, o con un coinvolgimento successivo dell'ufficio di Procura.

Nondimeno, il conflitto è per lo più potenziale, perché in concreto è proprio il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (il CNAI-PIC) a fare da cerniera tra i due organi, assicurando la sinergia tra investigazione amministrativa e attività di polizia giudiziaria.

## Bibliografia

APRATI, Roberta (2010): *La notizia di reato nella dinamica del procedimento penale* (Napoli, Jovene)

AZZARONE, Raffaele (2014a): “Cyber vademecum (Parte I)”, *Gnosis*, 1, pp. 62 – 76

AZZARONE, Raffaele (2014b): “Cyber vademecum (Parte II)”, *Gnosis*, 3, pp. 36 – 47

AZZARONE, Raffaele (2014c): “Cyber vademecum (Parte III)”, *Gnosis*, 4, pp. 34 – 46

AZZARONE, Raffaele (2015a): “Cyber vademecum (Parte IV)”, *Gnosis*, 2, pp. 88 – 98

AZZARONE, Raffaele (2015b): “Cyber vademecum (Parte V)”, *Gnosis*, 3, pp. 124 – 132

AZZARONE, Raffaele (2015c): “Cyber vademecum (Parte VI)”, *Evoluzione della minaccia*, *Gnosis*, 4, pp. 84 - 94

BARILE, PAOLO (1987): “DEMOCRAZIA E SEGRETO”, *QUADERNI COSTITUZIONALI*, 1, pp. 29 - 50

BIFULCO, RAFFAELE (2023): “VOCE SEGRETO E POTERE POLITICO”, in CARTABIA, Marta e RUOTOLO, Marco (editors): *Enc. dir., I tematici, V – Potere e Costituzione* (Milano, Giuffrè), p. 1096 - 1121

BONTEMPELLI, Manfredi (2009): *L'accertamento amministrativo nel sistema processuale penale* (Milano, Giuffrè)

BONZANO, Carlo (2008): “La nuova tutela penale del segreto di Stato: profili sostanziali e processuali. Commento a l. 3 agosto 2007 n. 124”, *Diritto penale e processo*, 1, pp. 24-35

BONZANO, Carlo (2010a): *Il Segreto di Stato nel processo penale* (Padova, Cedam)

BONZANO, Carlo (2010b): “La Consulta “suggerisce” una tutela oggettiva ed assoluta del segreto di Stato nel processo penale”, *Diritto penale e processo*, 16, 3, pp. 301 - 314

FERRO (2015), p. 53 ss. e MURRO (2023). Nell'ambito dell'aviazione civile, però, sono state messe a punto regole che valorizzano l'autonomia delle inchieste tecniche o di sicurezza sugli incidenti e l'impermeabilità della procedura giudiziaria rispetto agli esiti conoscitivi delle *safety investigations* (In argomento si rinvia a DI BITONTO (2017), p. 3804 ss.). Ad esempio, gli investigatori dell'ANSV possono accedere immediatamente e liberamente al luogo dell'incidente e, previa comunicazione al P.M., anche al luogo dove sono custodite le prove sottoposte a sequestro per esaminarle. Il previo accordo con il P.M. è previsto soltanto nell'ipotesi in cui debbano essere svolti accertamenti tecnici irripetibili e qualora la persona sottoposta alle indagini abbia fatto riserva di incidente probatorio: nel primo caso, il P.M. ha diritto di prendere parte all'atto e di concordare con l'ANSV le modalità tecniche dell'atto, devolvendo la risoluzione del conflitto al Presidente dell'ANSV e al Procuratore della Repubblica competente per le indagini. Niente di analogo, invece, pare essere previsto con riguardo alle investigazioni dell'Agenzia per la cybersicurezza.

<sup>55</sup> Secondo SALVI (2022), pp. 14-15, il problema della regolazione dei rapporti tra l'Agenzia cyber, il comparto di informazione per la sicurezza e l'autorità giudiziaria «non può essere affrontato in termini di primazia dell'accertamento penale, come forse un tempo si sarebbe fatto».

- BONZANO, Carlo (2011): “voce Segreto di Stato (Dir. Proc. Pen.)”, in GAITO, Alfredo (a cura di): *Digesto delle Discipline Penalistiche, Aggiornamento VI* (Torino, UTET), pp. 586 – 623
- BONZANO, Carlo (2022): “Matière pénale e diritto al silenzio: la Consulta mette un punto fermo ... o quasi”, *Diritto penale e processo*, 28, 1, pp. 47 – 60
- BONZANO, Carlo (2023): “Commento all’art. 270-bis c.p.p.”, in GIARDA, Angelo e SPANGHER, Giorgio (a cura di): *Codice di procedura penale commentato* (Milano, Wolters Kluwer), pp. 3649 – 3654
- BONZANO, Carlo (2023): “Commento all’art. 202 c.p.p.”, in GIARDA, Angelo e SPANGHER, Giorgio (editors): *Codice di procedura penale commentato I* (Milano, Wolters Kluwer), pp. 2860 – 2874
- CADOPPI, Alberto, CANESTRARI, Stefano, MANNA, Adelmo e PAPA, Michele eds (2019): *Trattato di Diritto penale. Cybercrime* (Torino, Giappichelli)
- CAIA, Giuseppe (2022): “voce Servizi di Informazione”, in *Enc. dir., I tematici, III – Funzioni Amministrative* (Milano, Giuffrè), pp. 1037 – 1052
- CAIA, Giuseppe e BRESCIANI, Pier Francesco (2021): “Le istituzioni della sicurezza in Italia”, in PANEBIANCO, Angelo (editor): *Democrazia e sicurezza. Società occidentali e violenza collettiva* (Bologna, Il Mulino), pp. 319 – 355
- CALIGIURI, Mario (2021): *Intelligence e diritto. Il potere invisibile delle democrazie* (Soveria Mannelli, Rubbettino)
- CALIGIURI, Mario (2016): “Il dilemma della cyber intelligence”, *Gnosis*, 2, pp. 22 – 29
- CANESCHI, Gaia (2020): “Nemo tenetur se detegere anche nei procedimenti amministrativi sanzionatori? La parola alla Corte di giustizia”, *Cassazione penale*, 2, pp. 579 – 587
- CAROTTI, Bruno (2020): “Sicurezza cibernetica e Stato-Nazione. Decreto legge 21 settembre 2019, n. 105, convertito con modificazioni dalla Legge 18 novembre 2019, n. 133”, *Giornale di diritto amministrativo*, 5, pp. 629 – 641
- CERRUTI, Alessandra (2013): “Delle condizioni soggettive dell’opposizione del segreto di Stato: vecchi problemi, nuovi bilanciamenti, medesimi limiti”, *Giurisprudenza Italiana*, 1, pp. 35 – 42
- CESARI, Claudia (1993): “Atti del procedimento amministrativo e processo penale tra limiti del codice e urgenze della prassi”, *Cassazione penale*, 1, pp. 143 – 145
- CESARI, Claudia (2021): “L’impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite”, *Revista Brasileira de Direito Processual Penal*, 3, pp. 1167 – 1187
- Conso, Giovanni (1979): “Relazione di sintesi”, in *Segreti e prova penale, Atti del Convegno di Studio Enrico De Nicola (Ferrara 1978)* (Giuffrè, Milano), pp. 195 – 211
- DE GENNARO, Gianni (2011): “Cultura della sicurezza e attuazione della riforma”, *Gnosis*, 2, pp. 3 – 14
- DE GENNARO, Gianni (2018): “Intelligence, imprese private e nuove tecnologie digitali”, in *I primi 20 anni: riflessioni sulla frontiera della conoscenza. Phronesis. Ventennale d’intelligence*, III, (Roma, Eurilink University press), pp. 83 – 94
- DELL’ANNO, Pierpaolo (2020): “Le attività di intelligence”, in SCALFATI, Adolfo (editor): *Pre-investigazioni (espediti e mezzi)* (Torino, Giappichelli), pp. 207 – 235
- DI BITONTO, Maria Lucia (2006): “Raccolta di informazioni e attività di intelligence”, in KOSTORIS, Roberto e ORLANDI, Renzo (editors), *Contrasto al terrorismo interno e internazionale* (Torino, Giappichelli), pp. 253 – 264

DI BITONTO, Maria Lucia (2017): “Professione medica e procedimento penale: le novità dopo la legge n. 24/2017”, *Cassazione penale*, 10, pp. 3799 - 3808

FERRO, Giovanni Battista, (2015): “L’inchiesta di sicurezza e l’inchiesta (rectius l’indagine) dell’autorità giudiziaria: una insopprimibile contradiction in adiecto?”, in FRANCHI, Bruno e VERNIZZI, Simone (editors): *Prevenzione degli incidenti aerei. La nuova normativa internazionale e dell’unione europea* (Torino, Giappichelli), pp. 53 - 60

FRANCHI, Bruno (2015): “Inchieste di sicurezza, indagini dell’Autorità giudiziaria: problematiche applicative del regolamento UE n. 996/2010”, in FRANCHI, Bruno e VERNIZZI, Simone (editors): *Prevenzione degli incidenti aerei. La nuova normativa internazionale e dell’unione europea* (Torino, Giappichelli), pp. 3 - 38

FUMU, Giacomo (1992): “Sub art. 220 disp. att. e coord.”, in CHIAVARIO, Mario (editor): *Commento al nuovo codice di procedura penale - la normativa complementare - II - Norme di coordinamento e transitorie* (Torino, Giappichelli) pp. 73 - 85

FURGIUELE, Alfonso (2020): “Le investigazioni extrapenali di natura “mista””, in SCALFATI, Adolfo (editor): *Pre-investigazioni (espediti e mezzi)* (Torino, Giappichelli), pp. 141 - 162

FURIN, Novelio (1999): “Diritto di difesa, indizi, sospetti e l’art. 220 disp. att. c.p.p.”, *Cassazione penale*, 9, pp. 1634 - 1635

GALANTINI, Novella (2022): “La circolazione della prova nei rapporti tra procedimento tributario e procedimento penale”, *Rivista italiana di diritto e procedura penale*, 3, pp. 999 - 1013

GALLUCCIO MEZIO, Gaetano (2023a): “Sub art. 220 disp. att. coord.”, in GIARDA, Angelo e SPANGHER, Giorgio (editors): *Codice di procedura penale commentato* (Milano, Wolters Kluwer), pp. 3712 - 3717

GALLUCCIO MEZIO, Gaetano (2023b): “Sub art. 223 disp. att. coord.”, in GIARDA, Angelo e SPANGHER, Giorgio (editors): *Codice di procedura penale commentato* (Milano, Wolters Kluwer), pp. 3725 - 3732

GAMBACURTA, Stefano (2008a): “I rapporti con altri soggetti”, in MOSCA, Carlo, GAMBACURTA, Stefano, SCANDONE, Giuseppe e VALENTINI, Marco (editors): *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)* (Milano, Giuffrè), pp. 281 - 338

GAMBACURTA, Stefano (2008b): “I rapporti con le Forze armate e le Forze di polizia”, in MOSCA, Carlo, GAMBACURTA, Stefano, SCANDONE, Giuseppe e VALENTINI, Marco (editors): *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)* (Milano, Giuffrè), pp. 304 - 323

GIUPPONI, Tommaso Filippo (2009): “Servizi di informazione e forze di polizia dopo la legge n. 124/2007”, in *Astrid Online*, pp. 1 - 10

GIUPPONI, Tommaso Filippo (2010a): “Servizi di informazione e segreto di stato nella legge n. 124/2007”, in CARIOLA, Agatino, CASTORINA, Emilio e CIANCIO, Adriana (editors): *Studi in onore di Luigi Arcidiacono, IV* (Torino, Giappichelli), pp. 1677 - 1751

GIUPPONI, Tommaso Filippo (2010b): “La riforma del sistema di informazione per la sicurezza della Repubblica”, in ILLUMINATI, Giulio (editor): *Nuovi profili del segreto di Stato e dell’attività di intelligence* (Torino, Giappichelli), pp. 53 - 128

GIUPPONI, Tommaso Filippo (2017): voce *Segreto di Stato (dir. cost.)*, in *Enc. dir., Annali*, X, 2 (Milano, Giuffrè), pp. 856 - 881

GIUPPONI, Tommaso Filippo (2023): “voce Sicurezza e potere”, in CARTABIA, Marta e RUOTOLO, Marco (editors): *Enc. dir., I tematici, V - Potere e Costituzione* (Milano, Giuffrè), pp. 1149 - 1173

GORI, Ugo (2014): “Le nuove minacce cyber”, *Informazioni della Difesa*, 6, pp. 5 - 29.

- GORI, Ugo (2016): “Interesse nazionale, intelligence e strategie nell’era cibernetica”, *Gnosis*, 2, pp. 86 – 93
- GREVI, VITTORIO (1978): “Segreto di Stato e processo penale. Evoluzione normativa e questioni ancora aperte”, in CHIAVARIO, MARIO (EDITOR): *SEGRETO DI STATO E GIUSTIZIA PENALE* (ZANICHELLI, BOLOGNA) 1978, PP. 225 - 250
- GREVI, VITTORIO (2012): “RAPPORT SUR LE SECRET ET LA PROCÉDURE EN DROIT ITALIEN (1976)”, IN GIULIANI, LIVIA (EDITOR), *SCRITTI SUL PROCESSO PENALE E SULL’ORDINAMENTO PENITENZARIO (1930)*, I, II (PADOVA, CEDAM), PP. 659 – 676
- JEMOLO, Arturo Carlo (1995): “Diritto d’informazione dello Stato (a proposito di una recente polemica)”, *Per Aspera Ad Veritatem*, 1, disponibile su <https://gnosis.aisi.gov.it/sito/Rivista1.nsf/ServNavig/2>
- KOSTORIS, Roberto E. (1964): *Il segreto come oggetto della tutela penale* (Padova, CEDAM)
- KOSTORIS, Roberto E. (1990): “Sub art. 220 disp. att. e coord.”, in AMODIO, Ennio e DOMINIONI, Oreste (editors): *Commentario del nuovo codice di procedura penale. Appendice-Norme di coordinamento e transitorie* (Milano, Giuffrè) pp. 73 - 85
- MAFFETTONI, Sebastiano e MELIDORO, Domenico (2015): “Democrazia e segreto”, *Gnosis*, 3, pp. 12 - 19
- MAZZA, Oliviero (2000): “L’utilizzabilità processuale del verbale di constatazione redatto dalla Guardia di Finanza”, *Corriere tributario*, 23, 18, pp. 1280 - 1287
- MONTAGNESE, Alfonso e NERI, Claudio (2016): *L’evoluzione della sicurezza nazionale in Italia*, in [sicurezzanazionale.gov.it](http://sicurezzanazionale.gov.it), disponibile su [www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/02/evoluzione-sicurezza-nazionale-Montagnese-Neri.pdf](http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/02/evoluzione-sicurezza-nazionale-Montagnese-Neri.pdf), pp. 1 - 55
- MORRONE, ANDREA (2010): “Il nomos del segreto di Stato”, in ILLUMINATI, Giulio (editor): *Nuovi profili del segreto di Stato e dell’attività di intelligence* (Torino, Giappichelli), p. 3 - 52
- MOSCA, Carlo (1985): “Segreto di Stato e attività dei Servizi di sicurezza”, *Rassegna della giustizia militare*, pp. 189 - 209
- MOSCA, Carlo (2012): *La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza* (Padova, Cedam)
- MOSCA, Carlo (2018): “Democrazia e sistema di intelligence negli ultimi quarant’anni. Profili normativi”, in *I primi 20 anni: riflessioni sulla frontiera della conoscenza. Phronesis. Ventennale d’intelligence*, III (Roma, Eurilink University press), pp. 23 - 44
- MOSCA, Carlo (2018a): “Il sistema di informazione per la sicurezza della Repubblica e le garanzie funzionali”, in CALIGIURI, Mario e VALENTINI, Marco (editors): *Materiali di intelligence. Dieci anni di studi 2007-2017* (Soveria Mannelli, Rubbettino), pp. 115 - 133
- MOSCA, Carlo (2018b): *Democrazia e intelligence italiana. Dieci anni dopo tra cultura, diritto e nuove sfide della democrazia* (Napoli, Editoriale Scientifica)
- MOSCA, Carlo (2019): “Segreto – Trasparenza”, *Gnosis*, 4, pp. 147 - 157
- MOSCA, Carlo, GAMBACURTA, Stefano, SCANDONE, Giuseppe e VALENTINI, Marco eds (2008), *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)* (Milano, Giuffrè)
- MURRO, Ottavia (2023): “Le inchieste dell’agenzia nazionale per la sicurezza del volo e i limiti all’attività della polizia giudiziaria”, *Diritto penale contemporaneo – Rivista Trimestrale*, questo numero
- NOBILI, Massimo (1984): “Atti di polizia amministrativa utilizzabili nel processo penale e diritto di difesa: una pronuncia marcatamente innovativa”, *Foro italiano*, 107, 2, pp. 375 - 379

- ORLANDI, Renzo (1992): *Atti e informazioni dell’Autorità amministrativa nel processo penale. Contributo allo studio delle prove precostituite* (Milano, Giuffrè)
- PACE, Alessandro (2015): *Stato costituzionale e segreto di Stato: una coesistenza problematica*, in *Giurisprudenza costituzionale*, 60, 5, pp. 1719 – 1738
- PAULESU, Pierpaolo (2023): “Sub art. 330 c.p.p.”, in GIARDA, Angelo e SPANGHER, Giorgio (editors): *Codice di procedura penale commentato* (Milano, Wolters Kluwer), pp. 1509 – 1521
- PISA, PAOLO (1977): “Il segreto di Stato di fronte alla Corte costituzionale: luci ed ombre in attesa della riforma”, *Giurisprudenza costituzionale*, 22, 1, pp. 1206 – 1214
- PIZZETTI, FRANCESCO (1978): “PRINCIPI COSTITUZIONALI E SEGRETO DI STATO”, in CHIAVARIO, Mario (editor), *Segreto di Stato e giustizia penale* (Zanichelli, Bologna), pp. 91 – 111
- PRESIDENZA DEL CONSIGLIO DEI MINISTRI (2013): *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, disponibile su [www.agid.gov.it/sites/default/files/repository\\_files/leggi\\_decreti\\_direttive/quadro-strategico-nazionale-cyber\\_0.pdf](http://www.agid.gov.it/sites/default/files/repository_files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf)
- RAMPIONI, Matteo (2019): “Le c.d. indagini “anfibie”: linee di fondo sul controverso legame tra attività ispettive e processo penale”, *Processo penale e giustizia*, 1, pp. 232 – 248
- RENZI, Andrea (2021): “La sicurezza cibernetica: lo stato dell’arte”, *Giornale di diritto amministrativo*, 4, pp. 538 – 548
- RICOTTA, Federico Niccolò (2023a): “Il segreto di Stato”, in COLAIACOVO, Guido (editor): *Sicurezza, Informazioni e Giustizia penale* (Pisa, Pacini Giuridica), in corso di pubblicazione
- RICOTTA, Federico Niccolò (2023b): “Il segreto di Stato nel processo penale”, in COLAIACOVO, Guido (editor): *Sicurezza, Informazioni e Giustizia penale* (Pisa, Pacini Giuridica), in corso di pubblicazione
- RIVELLO, Pierpaolo (2023a): “Sub Art. 256-bis c.p.p.”, in GIARDA, Angelo e SPANGHER, Giorgio (editors): *Codice di procedura penale commentato* (Milano, Wolters Kluwer), pp. 3381 – 3383
- RIVELLO, Pierpaolo (2023b): “Sub Art. 256-ter c.p.p.”, in GIARDA, Angelo e SPANGHER, Giorgio (editors): *Codice di procedura penale commentato* (Milano, Wolters Kluwer), pp. 3383 – 3385
- SALVI, Giovanni (2022), “Attuazione della giurisdizione penale nello spazio virtuale e sicurezza nazionale”, *Sistema penale*, pp. 1 – 16
- SALVI, Giovanni (2023): “Potere e intelligence”, in CARTABIA, Marta e RUOTOLO, Marco (editors): *Enc. dir., I tematici, V – Potere e Costituzione* (Milano, Giuffrè), pp. 248 – 279
- SCALFATI, Adolfo (2020): “Il fermento pre-investigativo”, in SCALFATI, Adolfo (editor): *Pre-investigazioni (espedienti e mezzi)* (Torino, Giappichelli), pp. 1 – 10.
- SCANDONE, Giuseppe (2008): *Il segreto di Stato nella legge di riforma*, in MOSCA, Carlo, GAMBACURTA, Stefano, SCANDONE, Giuseppe e VALENTINI, Marco (editors), *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)* (Milano, Giuffrè), pp. 499 – 558
- SFORZA, Ilaria (2022): “Il nemo tenetur se detegere nelle audizioni Consob e Banca d’Italia: uno statuto ancora da costruire”, *Sistema penale*, 2, pp. 83 – 104
- SORBELLO, Pietro (2016): “La valutazione di sospetti, indizi e notizie di reato nel passaggio (incerto) dalle attività ispettive alle funzioni di polizia giudiziaria”, *Diritto penale contemporaneo*, 2, pp. 125 – 135
- SPANGHER, Giorgio (1990): “Sub art. 202 c.p.p.”, in CHIAVARIO, Mario (editor), *Commento al codice di procedura penale* (Torino, UTET), pp. 469 – 474

UBERTIS, Giulio (1992): "L'utilizzazione dibattimentale di prelievi e analisi di campioni", *Cassazione penale*, 2, pp. 289 - 290

UBERTIS, Giulio (1995): "voce Prova in generale", in *Dig. disc. pen.*, Vol. X (Torino, UTET), pp. 296 - 338

VALENTINI, Marco (2008): *L'ordinamento del sistema politico dell'informazione per la sicurezza*, in MOSCA, Carlo, GAMBACURTA, Stefano, SCANDONE, Giuseppe e VALENTINI, Marco (editors), *I servizi di informazione e il segreto di Stato (Legge 3 agosto 2007, n. 124)* (Milano, Giuffrè), pp. 23 - 93



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>