

CJN

Diritto Penale Contemporaneo

RIVISTA TRIMESTRALE

REVISTA TRIMESTRAL DE DERECHO PENAL
A QUARTERLY REVIEW FOR CRIMINAL JUSTICE

3/2024

EDITOR-IN-CHIEF

Gian Luigi Gatta

EDITORIAL BOARD

Italy: Mitja Gialuz, Antonio Gullo, Guglielmo Leo, Luca Luparia, Francesco Mucciarelli, Francesco Viganò

Spain: Jaume 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, Teresa Bene, 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 Caveró, Loredana Garlati, Glauco Giostra, Víctor Gómez Martín, José Luis Guzmán Dalbora, Ciro Grandi, Giovanni Grasso, Giulio Illuminati, Roberto E. Kostoris, Máximo Langer, Juan Antonio Lascurain Sánchez, Maria Carmen López Peregrín, Sergio Lorusso, Ezequiel Malarino, Francisco Maldonado Fuentes, Stefano Manacorda, Juan Pablo Mañalich Raffo, Vittorio Manes, Grazia Mannozi, Teresa Manso Porto, Luca Marafioti, Joseph Margulies, Enrico Marzaduri, Luca Maserà, Jean Pierre Matus Acuña, Anna Maria Maugeri, Oliviero Mazza, Iván Meini, Alessandro Melchionda, Chantal Meloni, Melissa Miedico, Vincenzo Militello, 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 Quattrocchio, Tommaso Rafaraci, Paolo Renon, Lucia Risicato, Mario Romano, Maria Ángeles Rueda Martín, Carlo Ruga Riva, Stefano Ruggieri, Francesca Ruggieri, Dulce Maria Santana Vega, Marco Scoletta, Sergio Seminara, Paola Severino, Nicola Selvaggi, Rosaria Sicurella, Jesús Maria Silva Sánchez, Carlo Sotis, Andrea Francesco Tripodi, 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 2024 - CODICE ISSN 2240-7618 - Registrazione presso il Tribunale di Milano, al n. 554 del 18 novembre 2011.
Impaginazione a cura di Chiara Pavese

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. 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. 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. 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>CRIMINI DEI COLLETTI BIANCHI</p> <p><i>DELITOS DE CUELLO Y CORBATA</i></p> <p><i>WHITE COLLAR CRIMES</i></p>	<p>Codice della crisi d'impresa e bancarotta: appunti 1</p> <p><i>Crisis empresarial y regulación de la bancarrota: apuntes</i></p> <p><i>Business Crisis Code and Bankruptcy Crimes: Notes</i></p> <p>Alberto Alessandri</p>
<p><i>WHITE COLLAR CRIMES</i></p>	<p>Materialità e offensività dell'alterazione, investitore ragionevole e giudizi nella manipolazione del mercato 17</p> <p><i>Materialidad y Ofensividad de la Alteración, Inversor Razonable y Juicios en la Manipulación del Mercado</i></p> <p><i>Materiality and Harmfulness of the Alteration, Reasonable Investor, and Judgments in Market Manipulation</i></p> <p>Francesco Mucciarelli</p>
<p>DIRITTO PENALE E DIRITTI FONDAMENTALI</p> <p><i>DERECHO PENAL Y DERECHOS FUNDAMENTALES</i></p> <p><i>CRIMINAL LAW AND FUNDAMENTAL RIGHTS</i></p>	<p>"Planando sopra boschi di braccia tese": il saluto fascista davanti alle sezioni unite 87</p> <p><i>"Planeando sobre bosques de brazos extendidos": el saludo fascista ante las Secciones Unidas</i></p> <p><i>"Gliding Over Forests of Outstretched Arms": The Fascist Salute Before the Cassation's Joint Criminal Branches</i></p> <p>Alessandro Tesauro</p>
<p>DIRITTO PENALE E DIRITTI FONDAMENTALI</p> <p><i>DERECHO PENAL Y DERECHOS FUNDAMENTALES</i></p> <p><i>CRIMINAL LAW AND FUNDAMENTAL RIGHTS</i></p>	<p>La vita come "controlimite" all'autodeterminazione responsabile: denegata giustizia? 109</p> <p><i>La vida como "contra-límite" a la autodeterminación responsable: ¿justicia denegada?</i></p> <p><i>Life as a "Counter-Limit" to Responsible Self-Determination: Denied Justice?</i></p> <p>Roberto D'Andrea</p>

<p>DIRITTO PENALE COMPARATO</p> <p><i>DERECHO PENAL COMPARADO</i></p> <p><i>COMPARATIVE CRIMINAL LAW</i></p>	<p>La Svezia tra <i>Nordic exceptionalism</i> e politiche di <i>Crimmigration</i> 141</p> <p><i>Suecia entre el excepcionalismo nórdico y las políticas de crimmigración</i></p> <p><i>Sweden Between Nordic Exceptionalism and Crimmigration Policies</i></p> <p>Riccardo Ercole Omodei</p>
<p>IL FOCUS SU...</p> <p><i>EL ENFOQUE EN...</i></p> <p><i>FOCUS ON...</i></p>	<p>La <i>restorative justice</i> nel sistema della giustizia penale spagnola: peculiarità a confronto con il sistema italiano 156</p> <p><i>La justicia restaurativa en el sistema de justicia penal español: particularidades en comparación con el sistema italiano</i></p> <p><i>Restorative Justice in the Spanish Criminal Justice System: peculiarities compared with the Italian System</i></p> <p>Alice Pisconti</p>
<p>IL FOCUS SU...</p> <p><i>EL ENFOQUE EN...</i></p> <p><i>FOCUS ON...</i></p>	<p>Le nullità dell'imputazione tra quadro normativo nazionale e giurisprudenza europea 177</p> <p><i>Las nulidades de la imputación entre el marco normativo nacional y la jurisprudencia europea</i></p> <p><i>The Invalidities of the Accusation Between National Legislation and European Case Law</i></p> <p>Gianluca Varraso</p>
<p>IL FOCUS SU...</p> <p><i>EL ENFOQUE EN...</i></p> <p><i>FOCUS ON...</i></p>	<p>La "valutazione autonoma" della pericolosità nel sistema delle misure di prevenzione 203</p> <p><i>La "Evaluación Autónoma" de la Peligrosidad en el Sistema de Medidas de Prevención</i></p> <p><i>The "Autonomous Assessment" of Dangerousness in the Preventative Measures System</i></p> <p>Fabio Basile, Edoardo Zuffada</p>
<p>IL FOCUS SU...</p> <p><i>EL ENFOQUE EN...</i></p> <p><i>FOCUS ON...</i></p>	<p>Accesso abusivo a sistema informatico e conseguente rivelazione di segreto professionale 221</p> <p><i>Acceso indebido a un sistema informático o telemático y revelación de secreto profesional</i></p> <p><i>Unduly Access to a Computer or Telematic System and Disclosure of Professional Secrecy</i></p> <p>Davide Attanasio</p>

IL FOCUS SU...

EL ENFOQUE EN.....

FOCUS ON...

- 177 **Le nullità dell'imputazione tra quadro normativo nazionale e giurisprudenza europea**
Las nulidades de la imputación entre el marco normativo nacional y la jurisprudencia europea
The Invalidities of the Accusation Between National Legislation and European Case Law
Gianluca Varraso
- 203 **La "valutazione autonoma" della pericolosità nel sistema delle misure di prevenzione**
La "Evaluación Autónoma" de la Peligrosidad en el Sistema de Medidas de Prevención
The "Autonomous Assessment" of Dangerousness in the Preventative Measures System
Fabio Basile, Edoardo Zuffada
- 221 **Accesso abusivo a sistema informatico e conseguente rivelazione di segreto professionale**
Acceso indebido a un sistema informático o telemático y revelación de secreto profesional
Unduly Access to a Computer or Telematic System and Disclosure of Professional Secrecy
Davide Attanasio

Accesso abusivo a sistema informatico e conseguente rivelazione di segreto professionale*

Riflessioni a partire da un provvedimento della *High Court of Justice*

Acceso indebido a un sistema informático o telemático y revelación de secreto profesional

Unduly Access to a Computer or Telematic System and Disclosure of Professional Secrecy

DAVIDE ATTANASIO

Assegnista di ricerca in diritto penale presso l'Università degli Studi di Torino
davide.attanasio@unito.it

REATI INFORMATICI E A MEZZO
INTERNET

DELITOS INFORMÁTICOS

CYBERCRIMES

ABSTRACTS

Il lavoro origina da un provvedimento emesso dalla *High Court of Justice* britannica, chiamata a confrontarsi con la disciplina italiana dei reati di accesso abusivo a sistema informatico o telematico e di rivelazione di segreto professionale. Le questioni che meritano di essere approfondite sono due. La prima – che riguarda entrambi i delitti citati – concerne la funzione delle clausole di illiceità speciale nell'economia delle fattispecie incriminatrici. La seconda attiene invece all'oggettività giuridica del reato di cui all'art. 615-ter c.p., da tempo al centro delle riflessioni di dottrina e giurisprudenza e che, complice la continua evoluzione tecnologica, non ha tuttora trovato una definizione condivisa.

El artículo tiene su origen en una sentencia pronunciada por la *High Court of Justice* británica, en la que se analiza el marco jurídico italiano que regula los delitos de acceso indebido a un sistema informático o telemático y de revelación de secreto profesional. La sentencia plantea dos cuestiones que merecen ser examinadas en profundidad: la primera – que afecta a ambos delitos – se refiere a la función de las cláusulas especiales de ilegalidad en los tipos penales, mientras que la segunda dice relación con el bien jurídico protegido por el delito previsto en el artículo 615-ter del Código Penal italiano, un tema que ha sido largamente debatido tanto por la doctrina como por la jurisprudencia y que, debido a la continua evolución tecnológica, no acaba de encontrar una definición compartida.

The paper originates from a judgment issued by the British High Court of Justice, which addressed the Italian legal framework governing the offences of unduly access to a computer or telematic system and disclosure of professional secrecy. Two key issues arise. The first – pertaining to both of the aforementioned crimes – involves the function of special illegality clauses within the dimension of incriminating provisions. The second concerns the legal interest protected by the crime under Article 615-ter of the Italian Criminal Code, which has long been debated in legal scholarship and case law, and which, due to the ongoing technological evolution, still lacks a widely accepted definition.

* I riferimenti del provvedimento sono i seguenti: [2024] EWHC 1263 (Comm), disponibile sulla banca dati *Westlaw*, nonché liberamente accessibile sul sito web www.enterprisechambers.com.

SOMMARIO

1. Premessa: il diritto penale alle prese con la tecnologia. – 2. Introduzione sulle questioni giuridiche oggetto della vicenda. – 3. L'illiceità speciale del reato di cui all'art. 615-ter c.p.: la clausola "abusivamente". – 3.1 (segue) Il perimetro delle condotte tipiche: tra letture oggettive e riposizionamenti soggettivi della giurisprudenza. – 3.2. Loggettività giuridica: vecchie e nuove istanze di tutela. – 4. La nozione di giusta causa ai sensi dell'art. 622 c.p.: l'ordine dell'autorità britannica esclude la configurabilità del reato. – 5. Osservazioni conclusive.

1.

Premessa: il diritto penale alle prese con la tecnologia.

Le nuove tecnologie rappresentano, oramai da tempo, un vero e proprio banco di prova per tutti i formanti del diritto, che si trovano ad affrontare, con sempre maggiore frequenza, le continue e repentine evoluzioni dei processi tecnologici, nel corso degli anni ideati e sviluppati per i più svariati impieghi¹. Il legame tra tecnologia e diritto diviene ancora più complesso se si prende a riferimento il sistema penale, per sua natura strutturato per reagire a fatto compiuto. Lo *ius terribile*² – non potrebbe essere altrimenti – arriva dopo l'innovazione tecnologica: quando viene ad esistere un nuovo strumento o quando un dispositivo già noto è utilizzato per impieghi mai fatti sino a quel momento, soltanto allora insorge l'esigenza regolatoria del legislatore, la funzione accertativa (in ottica punitivo-sanzionatoria) del giudice – se la tecnologia è impiegata per finalità criminose – nonché il lavoro di sistematizzazione delle nuove questioni problematiche effettuato dalla dottrina.

È quello che sta avvenendo, volendo esemplificare, con gli algoritmi ad alta frequenza (c.d. *high-frequency trading* o HFT) nell'ambito degli abusi di mercato³ ovvero in tema di criptovalute che, nella dimensione penalistica, chiamano principalmente in causa fenomeni di matrice riciclatoria⁴.

Siffatto processo evolutivo è già avvenuto in relazione ai *computer crimes*, i quali rappresentano una delle sfere di tangenza più interessanti tra tecnologia e diritto penale. Intersezione quest'ultima, è solo il caso di accennarlo, che può assumere le più svariate sfaccettature. Impossibile – e poco utile ai fini del presente lavoro – provare a effettuarne una classificazione. Basti qui constatare che il legame può essere osservato tanto dall'angolo visuale del compimento di attività criminose⁵, quanto dalla prospettiva degli organi investigativi e accertativi⁶.

Il binomio tecnologia-diritto penale sarà qui indagato nella prospettiva dei menzionati reati informatici, introdotti nel codice penale con la l. 23 dicembre 1993, n. 547⁷, in recepimento della raccomandazione del Consiglio d'Europa⁸. Il provvedimento legislativo rappresenta uno dei primi e maggiormente significativi interventi di riforma nell'ambito della criminalità informatica⁹, finalizzato, come osservato in dottrina¹⁰, a fronteggiare il fenomeno dei c.d. *hackers*. L'art. 4, in particolare, ha aggiunto nella sezione del codice penale riservata all'inviolabilità del

¹ In argomento, già ALESSANDRI (1984), pp. 5 ss. e *passim*.

² Le osservazioni in merito alla relazione tra diritto penale e nuove tecnologie valgono, a ben vedere, anche con riguardo agli altri settori dell'ordinamento giuridico.

³ CONSULICH (2024), pp. 237 ss.; CONSULICH. (2018), pp. 195 ss. Si veda inoltre lo studio recentemente pubblicato sui quaderni Consob: CONSULICH *et al.* (2023).

⁴ BASILE (2024), pp. 453 ss.; CONSULICH (2022), pp. 153 ss.; PICOTTI (2018), pp. 590 ss.

⁵ Tale relazione può riflettersi nello strumento utilizzato per commettere uno o più reati (si pensi, per citarli nuovamente, agli HFT) o nel contesto (lo spazio virtuale) in cui il delitto si verifica (si immagini una truffa commessa per via telematica o una diffamazione a mezzo *social network*) o nell'oggetto materiale del reato (così, ad esempio, una recente sentenza della Corte di cassazione che ha ritenuto configurabile l'appropriazione indebita di file informatici; Cfr. Cass., sez. II, 10 aprile 2020, n. 11959, Rv. 278571-01). Per una nota critica alla sentenza citata, PISANI (2020), pp. 651 ss.

⁶ Le autorità investigative già da tempo utilizzano dispositivi tecnologici nell'ambito delle proprie attività d'indagine (si vedano, ad esempio, le intercettazioni informatiche o telematiche). Sull'utilizzo del captatore informatico, *ex multis*, CANESCHI (2019), pp. 417 ss. Più recente, invece, è il dibattito concernente l'utilizzo dell'intelligenza artificiale nell'amministrazione della giustizia e, in particolare, a fini eventualmente decisori. In argomento, *ex plurimis*, GIALUZ (2019); QUATTROCOLO (2022), pp. 533 ss. Significativa a riguardo l'adozione da parte dell'Unione europea del c.d. *AI Act* (regolamento (UE) 2024/1689), che marca un primo passo verso la regolazione dell'utilizzo dell'intelligenza artificiale nel sistema giustizia; cfr. BALSAMO (2024).

⁷ Per un commento alla l. n. 547/1993, MUCCIARELLI (1996), pp. 98 ss.; ROSSI (1994), pp. 427 ss.

⁸ Raccomandazione «*sur la criminalité en relation avec l'ordinateur*» del 13 settembre 1989, n. R (89) 9.

⁹ In argomento, già prima dell'entrata in vigore della legge citata, ALESSANDRI (1990), pp. 653 ss.; CORRIAS LUCENTE (1987), pp. 167 ss. e 519 ss. Si vedano poi, *ex multis*, i lavori di PICA (1999); PICOTTI (2000), pp. 1 ss.; PECORELLA (2006).

¹⁰ V., per tutti, PIERGALLINI (2015), p. 771.

domicilio un pacchetto di tre fattispecie incriminatrici¹¹, tutte costruite attorno alla tutela del sistema informatico o telematico da potenziali interferenze abusive ed eventualmente pregiudizievoli per la riservatezza dei dati in esso contenuti¹². Disposizione fulcro dei *computer crimes* – che sarà oggetto di approfondimento nel prosieguo – è l'art. 615-ter c.p., che disciplina il reato di accesso abusivo a sistema informatico/telematico protetto da misure di sicurezza. Tale norma è stata di recente interessata da una importante e più ampia novella legislativa, che ha modificato – in maniera a ben vedere draconiana – il trattamento sanzionatorio delle ipotesi aggravate di cui ai commi 2 e 3¹³.

Il presente lavoro affronta l'argomento accennato nella prospettiva di un provvedimento emesso dalla *High Court of Justice*¹⁴, trovatisi ad analizzare l'addentellato codicistico italiano – in specie l'art. 615-ter c.p. e, in via secondaria, l'art. 622 c.p. – nell'ambito di un procedimento esecutivo instaurato da parti attoree, persone giuridiche aventi sede nel Regno Unito, finalizzato al recupero delle somme ad esse dovute da un soggetto, condannato in conseguenza della violazione di doveri fiduciari nell'ambito dello svolgimento di attività lavorative¹⁵. Per quanto di interesse – e come meglio si descriverà *infra* (§ 2.) – il convenuto si opponeva alla richiesta emessa dall'autorità britannica¹⁶ di estrarre copia di taluni file asseritamente presenti nel sistema informatico a lui riconducibile (un personal computer e un cellulare), argomentando che in tal modo sarebbe incorso – unitamente al tecnico che si sarebbe dovuto occupare dell'estrazione dei dati – in una responsabilità penale ai sensi delle fattispecie incriminatrici richiamate¹⁷. Si riteneva infatti che nel sistema informatico avrebbero potuto essere presenti dati confidenziali riconducibili a società di cui il convenuto era stato in passato amministratore.

La prima questione su cui occorre soffermarsi concerne la configurabilità dell'accesso abusivo qualora all'interno del sistema informatico/telematico, di proprietà del potenziale soggetto attivo del reato, siano altresì presenti dati riferibili a persone terze. Il tema impone allora di soffermarsi sulla tipicità del delitto (§§ 3. e 3.1.) e sulla relativa oggettività giuridica (§ 3.2.).

La seconda questione attiene invece al ruolo della richiesta dell'autorità britannica (nelle forme del *Master McCloud order*) nell'economia del reato di cui all'art. 622 c.p., per la cui punibilità è necessaria, tra i vari elementi costitutivi, una rivelazione senza giusta causa (§ 4.).

Prima di scendere nel merito delle questioni, appare però utile fornire un sintetico inquadramento della vicenda, necessario per meglio comprendere la decisione cui perviene il giudice britannico.

2.

Introduzione sulle questioni giuridiche oggetto della vicenda.

Le questioni giuridiche di interesse originano, come anticipato in premessa, da un procedimento esecutivo instaurato per il recupero di talune somme che il convenuto era stato condannato a rifondere in favore delle parti attoree. Non avendo il debitore provveduto al pagamento, il creditore presentava un'ulteriore istanza ai sensi della *Part 71* delle *Civil Procedure Rules*, finalizzata a ottenere un ordine di presentazione del debitore in udienza affinché questo ultimo potesse fornire informazioni rilevanti ai fini dell'esecuzione della decisione¹⁸. È nell'ambito di tale procedimento che veniva emesso dall'autorità britannica l'ordine di estrarre copia di talune specifiche informazioni asseritamente contenute nel computer e nel cellulare del debitore convenuto (c.d. *McCloud Order*)¹⁹. In particolare, era necessario verificare se nei

¹¹ Si tratta degli artt. 615-ter, 615-quater e 615-quinquies c.p.

¹² La notazione chiama in causa il tema del bene giuridico tutelato dalle norme, su cui v. più approfonditamente *infra* § 3.2.

¹³ La cornice edittale della pena di cui al secondo comma, da uno a cinque anni, è stata innalzata a due-dieci anni, mentre quelle previste dal terzo comma sono state aumentate a tre-dieci e quattro-dodici anni, in forza dell'art. 16, l. 28 giugno 2024, n. 90, in materia di rafforzamento della *cybersicurezza* nazionale e di reati informatici.

¹⁴ Il provvedimento è stato emesso in data 24 maggio 2024 dalla sezione *Business and Property Courts of England and Wales, Commercial Court* (Mr. Justice Jacobs). Per i riferimenti, *supra* nt. 1.

¹⁵ § 5 del provvedimento.

¹⁶ C.d. *McCloud Order* (§ 19 del provvedimento). L'ordine veniva emesso al fine di dare seguito alle richieste avanzate dalle parti attoree nell'ambito del procedimento esecutivo.

¹⁷ §§ 1 ss. del provvedimento.

¹⁸ La *section 71.1* delle *Civil Procedure Rules* prevede: «*This Part contains rules which provide for a judgment debtor to be required to attend court to provide information, for the purpose of enabling a judgment creditor to enforce a judgment or order against him*».

¹⁹ In particolare, l'autorità richiedeva a un tecnico informatico di estrarre due copie dell'*hard drive* del computer e del cellulare. Una copia avrebbe dovuto essere consegnata alla difesa del convenuto, mentre la seconda sarebbe stata oggetto della ricerca dei file e delle informazioni specificate dal giudice. L'esperto ne avrebbe dunque dovuto stilare un elenco da consegnare alle difese (§ 19 del provvedimento commentato).

sistemi informatici fossero presenti alcuni file riferibili a nove società di cui il convenuto era stato amministratore.

Dato che i dispositivi si trovavano in Italia – anche il debitore aveva la propria residenza nel territorio italiano²⁰ – il giudice britannico si confronta con le fattispecie incriminatrici poste a tutela dell’inviolabilità del domicilio informatico (art. 615-ter c.p.) e della segretezza delle informazioni private (art. 622 c.p.). La difesa del convenuto ha sostenuto che, se si fosse dato corso al *McCloud Order*, il debitore, nonché legittimo proprietario dei dispositivi informatici, e l’esperto IT sarebbero andati incontro a una contestazione in sede penale, dapprima per l’accesso abusivo al sistema informatico e poi per la rivelazione delle informazioni ivi contenute.

Il dato fattuale dirimente, a parere della difesa del convenuto, risiedeva nella presenza all’interno dell’*hard drive* di computer e cellulare di dati e informazioni riservate, appartenenti alle nove società di cui il debitore era stato amministratore. Pertanto, valorizzando l’interesse giuridico della riservatezza e segretezza delle informazioni riferibili alle società, la difesa ha argomentato sulla configurabilità del reato di accesso abusivo a sistema informatico, sebbene quest’ultimo fosse di proprietà del convenuto destinatario del *McCloud Order*. La prima questione di interesse (su cui *infra*, § 3. ss.) si risolve allora nella ricostruzione del bene giuridico tutelato dalla fattispecie incriminatrice di cui all’art. 615-ter c.p.²¹. Non v’è chi non veda, infatti, che laddove si volesse declinare l’interesse tutelato nei termini della riservatezza delle informazioni contenute nel sistema informatico – e non tanto, o comunque non solo, nell’inviolabilità dello stesso: il delitto acquisterebbe dunque una natura plurioffensiva – la condotta di introduzione all’interno dei dispositivi per estrarre copia di file riferibili a soggetti terzi rispetto al proprietario del sistema potrebbe integrare il reato oggetto di scrutinio.

La seconda questione giuridica ruota invece attorno alla disposizione incriminatrice della rivelazione di segreto professionale²². Il dialogo tra le difese – le cui tesi non paiono per vero totalmente inconciliabili (*infra*, § 4.), diversamente dalle posizioni in tema di accesso abusivo: sembra infatti soccorrere, come si vedrà, la teoria c.d. mista – si incentra sulla definizione della clausola di illiceità espressa “senza giusta causa”, che, unitamente alla possibilità di verifica del nocimento, colora il tipo del reato (in specie la condotta di rivelazione). Entrambe le difese concordano nel ritenere che, ai fini della sussistenza della giusta causa, debba effettuarsi un bilanciamento degli interessi in gioco (qui: l’interesse patrimoniale di parte attorea a vedere eseguita la decisione di condanna emessa in suo favore e l’interesse delle società alla riservatezza, *ergo* alla *non disclosure* delle informazioni). Soltanto laddove il contro-interesse abbia portata pari o superiore a quello direttamente tutelato dalla norma incriminatrice potrebbe parlarsi di giusta causa. Sul punto, la difesa del convenuto ha sostenuto che l’interesse patrimoniale dell’attore non potesse prevalere su quello vantato dalle società. A ciò è stato pure aggiunto l’argomento della “necessità” – la cui sussistenza è stata esclusa dalla difesa del debitore – a mente del quale la rivelazione del segreto, per poter essere scriminata da una causa giusta, deve costituire l’unico strumento possibile per tutelare il contro-interesse.

Le motivazioni del provvedimento – conviene anticiparlo sin d’ora – depongono per la

²⁰ Alla luce del carattere transnazionale della vicenda, appare utile fare un cenno al tema del luogo di consumazione del reato di cui all’art. 615-ter c.p. e della relativa competenza territoriale. L’argomento, sebbene fosse stato sollevato dalla difesa delle parti attoree, non è stato specificamente affrontato dal giudice britannico (cfr. § 113 del provvedimento). Sulla più generale questione del *locus commissi delicti*, la Corte di cassazione a sezioni unite – facendo proprie talune argomentazioni di carattere tecnico-informatico in merito alla unicità o meno del sistema di elaborazione dei dati – ha affermato che il reato di accesso abusivo si consuma nel luogo ove si trova il soggetto che accede o si mantiene abusivamente nel sistema e non, invece, nel posto ove è locato il server. Cfr. Cass., sez. un., 24 aprile 2015, n. 17325, Rv. 263020, su cui, in senso critico, FLOR (2015), pp. 1291 ss. In termini adesivi alla pronuncia si esprimeva, già prima della pubblicazione delle motivazioni, BELLACOSA (2015). Quest’ultimo Autore analizza altresì l’ipotesi in cui il soggetto attivo del reato compia la condotta all’estero nei confronti di un sistema informatico ramificato in Italia (es. il reo accede dal proprio computer personale a un sistema informatico il cui server si trova in Italia). In casi del genere, osserva l’Autore da ultimo citato, potrebbe sostenersi che «l’azione criminosa, seppur compiuta dall’operatore senza allontanarsi fisicamente dalla postazione periferica, sia in realtà realizzata, secondo la dimensione digitale e immateriale dei fenomeni cibernetici, in parte all’estero e in parte, contemporaneamente, in Italia, con la conseguenza che il reato si potrebbe considerare comunque commesso nel territorio dello Stato italiano (cfr. art. 6, co. 2, c.p.), consentendo l’applicazione della disciplina della competenza per territorio prevista (ai sensi dell’art. 10, co. 3, c.p.p.) dalle regole generali ex art. 8 c.p.p. e dalle regole suppletive ex art. 9. c.p.p.». L’argomento difensivo che sembra essere stato sollevato nel procedimento inglese – ossia che non si sarebbe configurato alcun reato qualora computer e cellulari fossero stati trasferiti in Inghilterra e qui fosse stato effettuato l’accesso – non corrisponde tuttavia all’esempio proposto. Da quanto è dato comprendere dalle motivazioni del provvedimento, nella vicenda *de qua* non c’è uno sdoppiamento tra unità periferica di accesso (es. il computer) e sistema informatico inteso come oggetto materiale del reato. Gli unici dispositivi tecnologici di interesse sono il computer e il cellulare del debitore, alla cui parte *hardware* il tecnico informatico avrebbe dovuto fare accesso per estrarre copia di taluni dati ivi contenuti. Pertanto, qualora i menzionati dispositivi fossero stati portati all’estero, non vi sarebbe potuta essere alcuna proiezione offensiva della condotta nel territorio italiano.

²¹ Section D2 del provvedimento, §§ 61 ss.

²² Section D3 del provvedimento, §§ 93 ss.

non configurabilità di entrambe le fattispecie delittuose. È bene ora soffermarsi sulle questioni giuridiche anticipate, ripercorrendo le argomentazioni che emergono dal testo della decisione.

3. L'illiceità speciale del reato di cui all'art. 615-ter c.p.: la clausola "abusivamente".

Il perimetro applicativo della fattispecie incriminatrice è oggetto di dibattito in giurisprudenza e dottrina, ove vengono in rilievo orientamenti ondivaghi e talvolta contrastanti. Data per acquisita la definizione di sistema informatico o telematico²³ e di misure di sicurezza poste a protezione del dispositivo²⁴, la questione realmente problematica, per quanto qui di interesse, attiene alla delimitazione della condotta tipica. La norma prescrive due diversi comportamenti penalmente rilevanti: (i) l'introduzione abusiva nel sistema; (ii) il mantenimento all'interno dello stesso contro la volontà, espressa o tacita, di chi ha il diritto di escludere la permanenza di altri.

In particolare, l'elemento che colora la tipicità della condotta attiene alle modalità con cui essa si esplica, vale a dire "abusivamente". Ciò vale sia per la condotta di introduzione (*rectius* accesso²⁵), sia per quella di mantenimento all'interno del sistema. L'abusività del comportamento, pur se testualmente legata al solo comportamento di introduzione, si riflette altresì sulla condotta di trattenimento in contrasto con la volontà del titolare del sistema informatico/telematico. Nel primo caso (*id est* quello dell'introduzione), la nota di abusività si colloca a monte dell'ipotetica vicenda fattuale, vale a dire quando il soggetto accede al sistema senza autorizzazione; nel secondo, invece, l'accesso è originariamente legittimo, divenendo abusivo (*rectius* è la permanenza a divenire abusiva) in un secondo momento, ossia laddove venga meno l'autorizzazione concessa precedentemente o qualora le attività poste in essere dal soggetto attivo eccedano il perimetro definito dalla predetta autorizzazione²⁶.

Così preliminarmente inquadrato il concetto di abusività – relativo tanto alla introduzione, quanto alla permanenza nel sistema informatico – prima di tornare a confrontarsi più direttamente con il testo del provvedimento in analisi, appare utile effettuare una notazione ulteriore sull'avverbio "abusivamente". Secondo taluni, infatti, la formula normativa rappresenterebbe un mero espediente linguistico per richiamare l'attenzione (del giudice) sull'antigiuridicità

²³ In dottrina, per tutti PIERGALLINI (2015), p. 778. L'Autore ricorda come per sistema informatico debba intendersi «il complesso degli elementi fisici e logici che compongono un apparato di elaborazione automatizzato: dunque, tra gli altri, l'*hardware* e il *software*». Il sistema telematico è invece costituito da un «apparato, diverso dai servizi telefonici e telegrafici convenzionali, per la comunicazione a distanza di dati tramite strumenti informatici e mezzi di telecomunicazione [...]». Il sistema telematico è un sistema integrato, capace di gestire dati, voci, testi e immagini». V. inoltre MANTOVANI F. (2022), p. 614. In giurisprudenza, v. da ultimo Cass., sez. V, 27 giugno 2023, n. 27900, Rv. 284873-01, ove si descrive il sistema informatico (e telematico) come un insieme di «apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate – per mezzo di un'attività di "codificazione" e "decodificazione" – dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente».

²⁴ Può trattarsi di misure di sicurezza di natura logica (es. codici di accesso al sistema informatico) o fisica (chiavi metalliche per l'accensione di un dispositivo). Non è richiesta una particolare complessità delle misure – può essere anche una semplice password – né tantomeno deve verificarsi, ai fini della consumazione del reato, l'aggravamento delle stesse. Difatti, è la stessa disposizione che prevede la configurabilità del delitto qualora il soggetto sia legittimamente in possesso delle chiavi di accesso al sistema (non potrebbe dunque riscontrarsi alcun tipo di aggravamento), ma successivamente vi si mantenga all'interno contro la volontà di chi ha il diritto di escluderlo. Discussa è invece la possibilità di includere nella nozione di misure di sicurezza anche quegli accorgimenti di natura organizzativa esterni al sistema informatico in senso stretto (es. le chiavi di accesso ai locali ove è installato il sistema informatico). A riguardo, valorizzando la *ratio* complessiva della norma, posta a tutela del sistema informatico/telematico e non dei locali ove esso è contenuto, pare preferibile ritenere che per misure di sicurezza debbano intendersi esclusivamente quelle, di carattere logico o fisico-materiale, interne al sistema informatico. Per una panoramica di tutte le questioni citate in questa nota, cfr. PECORELLA (2021), pp. 2052 ss.

²⁵ Parte della dottrina ha osservato come sarebbe stato preferibile descrivere la condotta con il termine "accesso", anziché "introduzione". Quest'ultimo lemma, infatti, sembrerebbe meglio attagliarsi a condotte di superamento fisico di un perimetro, sulla falsariga di quanto si verifica nel caso della violazione di domicilio rilevante ai sensi dell'art. 614 c.p. Sul punto, CAPPELLINI (2022), p. 6729. Si veda, inoltre, SALVADORI (2023), pp. 704-705. Quest'ultimo Autore osserva come «il fatto tipico di "introdursi" in un sistema informatico deve sostanziarsi in un dialogo logico (o automatizzato) con la sua parte software. L'accesso si configura pertanto nel momento in cui il sistema informatico altrui esegue una data operazione, richiestagli dal soggetto agente mediante una serie di comandi, mettendolo nelle condizioni di poter operare e anche conoscere quanto in esso contenuto». Nella prassi, in termini sostanzialmente analoghi, Cass., sez. V, 1° ottobre 2008, n. 37322, in *Onelegale*.

²⁶ MANTOVANI F. (2022), p. 614 parla infatti di «mantenimento abusivo».

della condotta, non aggiungendo alcunché alla portata della fattispecie incriminatrice²⁷. In altre parole, l'esponente terminologico non farebbe altro che ribadire un canone basilare nel processo di accertamento del reato, vale a dire che non devono sussistere cause di esclusione dell'antigiuridicità. Volendo richiamare una già risalente ripartizione dogmatica, il lemma "abusivamente" sarebbe una clausola di illiceità (o antigiuridicità) espressa, ma non speciale²⁸.

La tesi che vede nel termine "abusivamente" una superfetazione linguistica non persuade invero sino in fondo. Non tanto per una ragione afferente alle tecniche legislative di formulazione delle norme – secondo cui ciascun esponente testuale dovrebbe avere un proprio significato specifico – bensì per un'argomentazione concernente la tipicità dell'illecito penale. L'incriminazione della condotta – introduzione o mantenimento nel sistema – si giustifica proprio in funzione del carattere di abusività, in assenza del quale il comportamento descritto dalla norma sarebbe pienamente lecito²⁹. La valutazione sull'illiceità della condotta entra dunque nel tipo del reato, assumendo una dimensione differente rispetto a quella confinata nel giudizio sull'antigiuridicità in senso stretto. La clausola normativa menzionata nell'art. 615-ter c.p. svolge allora la funzione di delimitare la rilevanza penale del comportamento³⁰.

In definitiva, la formula linguistica "abusivamente" concentra il disvalore della condotta tipica, esprimendo un giudizio di relazione tra la fattispecie incriminatrice e le regole extra-penalistiche che stabiliscono le condizioni di accesso al sistema informatico/telematico³¹. Qualora l'introduzione o la permanenza nel sistema si pongano in contrasto con i limiti fissati dalle prescrizioni autorizzatrici – che dipendono dalla volontà del titolare del dispositivo – allora la condotta si dirà abusiva e, quindi, penalmente rilevante.

Una siffatta interpretazione della clausola "abusivamente" si riverbera direttamente sui contorni della tipicità del reato, su cui ora occorre spendere qualche notazione ulteriore.

3.1. *(segue) Il perimetro delle condotte tipiche: tra letture oggettive e riposizionamenti soggettivi della giurisprudenza.*

Tanto chiarito sul ruolo che la clausola di illiceità svolge all'interno dell'art. 615-ter c.p., conta ora effettuare un ulteriore passo in avanti nell'esegesi della disposizione, utile per inquadrare il percorso argomentativo del giudice britannico, il quale – lo si ricorda (*supra*, § 2.) – è stato chiamato a confrontarsi con una vicenda fattuale peculiare: all'interno del sistema informatico oggetto del *McCloud Order* – la cui titolarità era del destinatario del provvedimento – avrebbero potuto essere presenti dati confidenziali riferibili a soggetti terzi.

Se il carattere abusivo della condotta racchiude il disvalore dell'illecito penale e se il comportamento tipico consiste nell'introdursi o mantenersi nel sistema informatico/telematico, vuol dire che la penale rilevanza del fatto si esaurisce nel momento in cui viene posta in essere la condotta abusiva. In altre parole, ciò che conta ai fini della configurazione del reato è la sussistenza dell'abusività quando il soggetto attivo si introduce o si mantiene nel sistema, non rilevando invece l'eventuale illiceità dei fatti compiuti successivamente all'istante di verifica della condotta³². Abusività e condotta – che in sé considerata ha valore neutro, non penalmente rilevante – si legano a doppio filo nella descrizione del tipo d'illecito. Ne consegue

²⁷ Tra gli Autori già citati, questa tesi è sostenuta da MANTOVANI F. (2022), p. 613; PIERGALLINI (2015), p. 776. Si vedano, inoltre, GATTA (2022), p. 486; PICA (1999), pp. 38 ss.

²⁸ La distinzione è di LEVI (1938), pp. 351 ss.; più recentemente ripresa e approfondita da PULITANÒ (1967), pp. 65 ss. e, in particolare, 68 ss. Stando alla teorizzazione di Levi, illustrata altresì da Pulitanò, la categoria della illiceità espressa si risolve nell'utilizzo esplicito di espressioni quali "illegittimamente", "abusivamente", etc.; l'illiceità speciale, invece, riflette la contrarietà di un elemento della fattispecie con una norma diversa da quella incriminatrice. Le due categorie, sottolineano gli Autori, non si sovrappongono completamente: può darsi il caso che un reato sia a illiceità espressa, ma non anche a illiceità speciale e viceversa. Sull'argomento, si rinvia inoltre al lavoro monografico di MORGANTE (2002), *passim* e, per le tesi di Levi e Pulitanò, pp. 27 ss. Nella manualistica, da ultimo, PIERGALLINI (2024), pp. 259 ss., che affronta il tema nella dimensione dell'errore sul fatto *ex art.* 47, co. 3 c.p.

²⁹ SALVADORI (2023), pp. 707 ss.

³⁰ MORGANTE (2002), pp. 139 ss. riconosce negli elementi di illiceità speciale la funzione delimitatrice del penalmente rilevante.

³¹ Nuovamente, SALVADORI (2023), p. 708. L'Autore osserva come l'abusività sia «una formula di sintesi mediante la quale il legislatore ha voluto dare espresso rilievo al conflitto intersoggettivo di interessi che costituisce l'essenza del reato di accesso abusivo ad un sistema informatico o telematico. Le condotte di introduzione e di mantenimento in un sistema informatico sono di per sé lecite, ma diventano abusive e, quindi, penalmente rilevanti, in base a valutazioni extrapenalistiche».

³² Cass., sez. un., 7 febbraio 2012, n. 4694, Rv. 251269. Per un commento, BARTOLI (2012), pp. 123 ss.; nonché, più diffusamente, FLOR (2012), pp. 126 ss. Per alcune riflessioni ulteriori, che prendono altresì in considerazione il contrastante orientamento fatto proprio dalle Sezioni Unite nel 2017 (Cass., sez. un., 8 settembre 2017, n. 41210, Rv. 271061), SEMINARA (2018), pp. 235 ss.

che la valutazione sulla penale rilevanza del fatto – *rectius* dell'abusività della condotta, che, come osservato, delimita l'ambito applicativo della fattispecie incriminatrice – verte sulla natura oggettiva dell'abusività e non, come pure sostenuto dalla giurisprudenza di legittimità³³, su profili di carattere soggettivo.

In particolare, il contenuto oggettivo dell'abusività è perimetrato in funzione delle prescrizioni³⁴ imposte dal titolare del dispositivo, dalla cui volontà – elemento quest'ultimo richiamato esplicitamente dalla norma – dipendono le modalità di accesso e permanenza all'interno del sistema informatico/telematico. La volontà del soggetto titolare si riflette tanto sull'opposizione delle misure di sicurezza³⁵ – qui prende corpo la condotta di introduzione eludendo i dispositivi di sicurezza del sistema (*rectius* in assenza originaria di autorizzazione) – quanto sull'eventuale revoca del permesso ad accedere o sulla perimetrazione delle attività consentite all'interno del sistema (qui viene in rilievo il «mantenimento abusivo»³⁶).

La lettura soggettivistica della fattispecie incriminatrice³⁷ – oltre a porsi in aperto contrasto con la lettera della legge: nella norma non v'è alcun riferimento alle finalità del soggetto attivo – non trova neppure conforto nella sua *ratio*. Nella relazione di accompagnamento del d.d.l. che prevedeva l'introduzione dell'accesso abusivo a sistema informatico nel codice penale si osservava come la «tutela [*fosse*] limitata ai sistemi informatici o telematici protetti da misure di sicurezza perché, dovendosi tutelare il diritto di uno specifico soggetto, è necessario che quest'ultimo abbia dimostrato, con la predisposizione di mezzi di protezione sia logica che fisica (materiale o personale) di voler espressamente riservare l'accesso e la permanenza nel sistema alle persone da lui autorizzate»³⁸. Ciò consente di constatare che l'abusività della condotta dipende dalla volontà del titolare del sistema, *ergo* dall'autorizzazione (e dal relativo contenuto) dallo stesso concessa in favore di altri individui. A nulla rilevando, invece, le finalità perseguite dal soggetto attivo del reato, la cui valorizzazione esegetica modificherebbe arbitrariamente il tipo dell'illecito. Si darebbe vita a un ambito applicativo decisamente più incerto e indeterminato, dato che la configurazione del reato dipenderebbe dall'accertamento di finalità appartenenti alla sfera interiore di colui che agisce.

A tacere infine degli effetti irragionevoli che si verrebbero a creare: come osservato in giurisprudenza, infatti, «se dovesse ritenersi che, ai fini della consumazione del reato, basti l'intenzione, da parte del soggetto autorizzato all'accesso al sistema informatico ed alla conoscenza dei dati ivi contenuti, di fare poi un uso illecito di tali dati, ne deriverebbe l'aberrante conseguenza che il reato non sarebbe escluso neppure se poi quell'uso, di fatto, magari per un ripensamento da parte del medesimo soggetto agente, non vi fosse più stato»³⁹.

Il rifiuto della tesi soggettivistica si coglie anche nel provvedimento qui commentato, nella parte in cui il giudice britannico esclude la configurabilità dell'art. 615-*ter* c.p. anche qualora il debitore convenuto (l'ipotetico soggetto attivo del reato) avesse avuto l'intenzione, nell'accedere al proprio sistema informatico, di visualizzare i dati riferibili alle società di cui egli era stato amministratore in passato⁴⁰.

Tale ricostruzione in punto di tipicità del reato, accolta (anche) dal giudice britannico, consente ora di guardare, a ritroso, la restante parte delle motivazioni del provvedimento,

³³ Cass., sez. un., 8 settembre 2017, n. 41210, cit., su cui criticamente FASANI (2017), pp. 1397 ss., nonché, nuovamente, SEMINARA (2018), pp. 235 ss. Sulla sentenza citata, inoltre, FLOR (2018), pp. 506 ss. Occorre specificare che la Corte di cassazione a sezioni unite, nel caso di specie, era stata chiamata a pronunciarsi sul disposto del co. 2, n. 1 dell'art. 615-*ter* c.p., vale a dire quando la condotta è posta in essere dal pubblico ufficiale o dall'incaricato di pubblico servizio. La questione di diritto sottoposta alla Suprema Corte era la seguente: «Se il delitto previsto dall'art. 615-*ter* c.p., comma 2, n. 1, sia integrato anche nella ipotesi in cui il pubblico ufficiale o l'incaricato di pubblico servizio, formalmente autorizzato all'accesso ad un sistema informatico o telematico, ponga in essere una condotta che concreti uno sviamento di potere, in quanto mirante al raggiungimento di un fine non istituzionale, pur in assenza di violazione di specifiche disposizioni regolamentari ed organizzative».

³⁴ Prescrizioni che, come rilevato in giurisprudenza, possono essere contenute in «disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro»; cfr. Cass., sez. un., 7 febbraio 2012, n. 4694, cit.

³⁵ In questo senso, la previsione delle misure di sicurezza può essere intesa come manifestazione della volontà del titolare di negare l'accesso ad altri; così MUCCIARELLI (1996), p. 99. Secondo taluni, inoltre, le misure di protezione svolgerebbero altresì la funzione di responsabilizzare la vittima (*id est* il titolare del sistema informatico). Per quest'ultima osservazione, PECORELLA (2006), pp. 324 ss.

³⁶ MANTOVANI F. (2022), p. 614.

³⁷ Valorizzata in Cass., sez. un., 8 settembre 2017, n. 41210, cit.

³⁸ Relazione di accompagnamento del d.d.l. n. 2773, dal titolo «Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica» (XI Legislatura, divenuto l. 23 dicembre 1993, n. 547), consultabile in www.camera.it.

³⁹ Cass., sez. V, 17 gennaio 2008, n. 2534, Rv. 239105. Argomentazione poi richiamata da Cass., sez. un., 7 febbraio 2012, n. 4694, cit., nonché ripresa in dottrina da SEMINARA (2018), p. 246.

⁴⁰ § 90 del provvedimento. Si legge quanto segue: «*Even if [defendant's] intention, when he accessed his own machines, was to look at confidential data of the companies, or disclose it to another person, the case-law indicates that this would not amount to an offence under Article 615-*ter*. As the Supreme Court of Cassation said, "the aims and purposes which may have subjectively led to access to the system are irrelevant".*

incentrate sull'individuazione del bene giuridico tutelato.

3.2. *L'oggettività giuridica: vecchie e nuove istanze di tutela.*

Prima di scendere nel merito del principale argomento approfondito dal giudice britannico⁴¹ – ossia il bene giuridico tutelato dal reato di cui all'art. 615-ter c.p. – conviene chiarire una questione di carattere tecnico, ancor prima che giuridico, utile per inquadrare l'oggetto materiale del delitto, nonché il relativo interesse tutelato.

L'autorità straniera, analizzando talune sentenze della Corte di cassazione, tratteggia, se mai ve ne fosse stato bisogno, la differenza tra sistema informatico/telematico e dati/informazioni ivi contenute⁴². La Suprema Corte afferma da tempo che il sistema informatico o telematico è «un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche»⁴³, mentre i dati sono «rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse»⁴⁴. Il sistema rappresenta dunque la parte *hardware* e/o *software* che raccoglie, utilizza o elabora dati, mentre questi ultimi sono le unità informatiche, costituite da bit, presenti all'interno del dispositivo. Ciò consente peraltro di distinguere il dato dall'informazione, che, volendo sintetizzare, costituisce il risultato comunicativo del dato. Le informazioni – per riprendere nuovamente le parole della Corte di cassazione – «sono costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente»⁴⁵.

Tale notazione preliminare permette di fissare un primo concetto basilare: nella dimensione delle nuove tecnologie, dati e sistema sono due cose differenti. E, come emerge chiaramente dalla lettura dell'art. 615-ter c.p., l'oggetto materiale del reato è il sistema e non il dato. La condotta tipica esplica i propri effetti sul primo e non sul secondo.

Ciò non basta, ad ogni modo, per esaurire il ragionamento giuridico-normativo sull'interesse protetto dalla norma in questione. In proposito, le posizioni sviluppate da dottrina e giurisprudenza presentano numerose sfaccettature⁴⁶. A tacere di opinioni minoritarie⁴⁷, il panorama è conteso principalmente da due orientamenti⁴⁸, che emergono anche dalla lettura del provvedimento in analisi⁴⁹.

Un primo orientamento – accolto in maniera pressoché costante in giurisprudenza⁵⁰ – ritiene che il bene giuridico debba essere individuato nella tutela del domicilio informatico. Ciò trova conforto nella collocazione sistematica del delitto in questione – inserito nella sezione dei delitti contro l'inviolabilità del domicilio – nonché nella descrizione delle condotte sulla falsariga della violazione di domicilio di cui all'art. 614 c.p. Un ulteriore argomento a sostegno di questa tesi si rinviene nella relazione di accompagnamento al disegno di legge che ha portato all'introduzione dell'art. 615-ter c.p., laddove si osservava che i sistemi informatici/telematici costituiscono «un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 del codice penale»⁵¹.

⁴¹ *Ibidem*, §§ 65 ss.

⁴² *Ibidem*, §§ 78-79. Così nelle motivazioni del provvedimento: «Accordingly, in my view, the court was (as in the previous case) drawing the distinction (which to my mind is fairly obvious) between the computer system which was a "set of devices", and the data which was stored on the system or which could be generated by that system. I note in passing that a similar approach, and formulation of the legal position, can be found in another Supreme Court of Cassation case (11689 of 2007)».

⁴³ Cass., sez. II, 17 giugno 2019, n. 26604, in *Onelegale*.

⁴⁴ *Ibidem*. Analogamente, Cass., sez. V, 27 giugno 2023, n. 27900, cit.; già Cass., sez. V, 20 marzo 2007, n. 11689, in *Onelegale*. Spunti in questo senso vengono altresì da Cass., sez. II, 10 aprile 2020, n. 11959, cit., pur nella sua criticabile interpretazione, ai fini del reato di appropriazione indebita, del file informatico come cosa mobile. In argomento, PAGELLA (2021).

⁴⁵ Cass., sez. II, 17 giugno 2019, n. 26604, cit.

⁴⁶ FLOR (2017).

⁴⁷ MANTOVANI M.O. (1994), pp. 17 ss. Ad avviso dell'Autore, la norma avrebbe di mira la tutela dell'integrità dei dati e dei programmi informatici. In tal modo, tuttavia, si creerebbe un'indebita sovrapposizione tra il bene giuridico protetto dall'art. 615-ter c.p. e quello tutelato dai reati di danneggiamento informatico.

⁴⁸ Per una sintesi delle varie posizioni, MINO (2016), pp. 487 ss.

⁴⁹ Cfr. in particolare gli argomenti proposti dalle parti, §§ 62 ss.

⁵⁰ Cass., sez. V, 27 giugno 2023, n. 27900, cit.; Cass., sez. II, 17 giugno 2019, n. 26604, cit.; Cass., sez. V, 8 giugno 2020, n. 17360, in *Dejure*; già Cass., sez. V, 6 dicembre 2000, n. 12732, Rv. 217743. FIANDACA e MUSCO (2020), p. 363; ROSSI (1994), pp. 435 ss.; cfr., inoltre, PLANTAMURA (2017), pp. 185 ss.

⁵¹ Per i riferimenti della relazione, *supra* nt. 39.

Un secondo orientamento, accolto perlopiù in dottrina⁵², facendo leva sull'impossibilità di paragonare il domicilio tradizionalmente inteso (in termini fisico-materiali) a quello informatico sostiene invece che l'interesse tutelato consista nella riservatezza dei dati e dei programmi contenuti nel sistema. Ne deriva che, qualora il dispositivo tecnologico non contenga alcun dato, in ossequio al principio di offensività il reato non potrebbe dirsi integrato⁵³.

Entrambe le tesi non convincono sino in fondo. La prima perché – come sottolineato da chi sostiene l'orientamento sulla riservatezza dei dati e non (soltanto) del sistema⁵⁴ – il domicilio tradizionalmente inteso e quello informatico presentano caratteristiche troppo differenti per essere assimilati ai fini dell'individuazione del bene giuridico tutelato. Il secondo orientamento – pur apprezzandosi nel tentativo di fornire un'esegesi maggiormente aderente all'evoluzione delle tecnologie e, in particolare, dei sistemi informatici/telematici totalmente smaterializzati – non si concilia con il dato testuale della norma che, come già osservato (*supra*, §§ 3. e 3.1.), parla di introduzione o mantenimento abusivo all'interno di un sistema informatico o telematico. Non v'è alcun riferimento ai dati o programmi ivi contenuti.

Sembra allora preferibile un'impostazione che individui l'interesse protetto dalla disposizione incriminatrice, sì nella riservatezza, ma non dei dati singolarmente considerati, bensì dell'intero sistema informatico/telematico, di cui il titolare ha diritto di godere senza interferenze altrui e rispetto al quale – come conferma l'elemento della necessaria apposizione delle misure di sicurezza – ha la facoltà di inibire o escludere soggetti terzi dall'accesso. In altre parole, l'art. 615-ter c.p. intende garantire, in capo al titolare, la libera ed esclusiva fruizione del proprio spazio virtuale, da non intendere nella sua materialità come avverrebbe nel caso della tutela del domicilio tradizionale⁵⁵. E ciò indipendentemente dal fatto che all'interno del sistema siano o meno contenuti dati o che, come nel caso di specie, la loro natura sia confidenziale perché riferibili a soggetti terzi. Del resto, anche l'accesso a un sistema informatico vuoto avrebbe un disvalore apprezzabile penalmente: non soltanto si direbbe violata la sfera (virtuale) personale dell'individuo titolare, ma l'ingresso nel sistema minerebbe intrinsecamente la sua riservatezza (e sicurezza), aumentando il rischio di nuovi e reiterati accessi (eventualmente finalizzati a carpire i dati che potrebbero essere caricati in futuro sul dispositivo).

L'identificazione del bene giuridico tutelato dall'art. 615-ter c.p. nella riservatezza informatica dello spazio virtuale (*ergo* della sua libera fruizione da parte del titolare che lo possiede) trova solida conferma – non tanto, o comunque non primariamente, nell'argomentazione teleologica⁵⁶ – ma soprattutto nel dato testuale della disposizione. Come già osservato, la tutela giuridica è circoscritta ai soli sistemi informatici protetti da misure di sicurezza: il legislatore penale ha dunque ritenuto di privilegiare esclusivamente quei sistemi rispetto ai quali il legittimo titolare ha manifestato la volontà che restino riservati. La condotta abusiva, poi, diviene tale qualora posta in essere contro la volontà del soggetto titolare, così avvalorando ulteriormente l'idea che l'interesse protetto dalla norma converga sulla riservatezza del sistema informatico/telematico, la cui operatività dipende dalle prescrizioni impartite dal titolare, dunque dalla volontà di quest'ultimo che il sistema venga utilizzato secondo specifiche condizioni. La tutela dei dati contenuti all'interno del dispositivo resta dunque fuori dal perimetro applicativo della fattispecie incriminatrice.

Conclusivamente – e per tornare al caso di specie – il giudice britannico, valorizzando la diversità tecnica tra sistema e dato, nonché ricostruendo il bene giuridico in termini di riservatezza informatica del primo e non del secondo ivi contenuto, accoglie la tesi sostenuta dalle parti attoree: il titolare del computer e del cellulare e il tecnico informatico deputato all'estrazione dei file, se avessero adempiuto alle richieste formulate nel *McCloud Order*, non sarebbero

⁵² PIERGALLINI (2015), pp. 772-773, ad avviso del quale «è del resto risaputo che l'accesso abusivo ad un sistema informatico ha quasi sempre come obbiettivo l'acquisizione di dati o materiali contenuti nell'elaboratore e il fatto che la tutela copra solo quei sistemi protetti da "misure di sicurezza" sta a significare che la tutela non rivela una operatività illimitata». Analogamente, MANTOVANI F. (2022), p. 615.

⁵³ PECORELLA (2021), p. 2055.

⁵⁴ PIERGALLINI (2015), p. 772.

⁵⁵ SALVADORI (2023), pp. 698 ss. e 728-729. In tal senso cfr. già PICOTTI (2000), pp. 6 e 22; nonché PICOTTI (2004), pp. 77 ss. e pp. 80-82. Questa sembra essere altresì la tesi sostenuta dalla difesa delle parti attoree nella vicenda *de qua* e accolta dal giudice britannico (cfr. in particolare §§ 68 ss. e 86 ss. del provvedimento, ove può leggersi: «[...] *What was protected was the owner's interest in exclusive access to an IT space, regardless of the nature of the information stored, and the free availability of the same against unlawful interference by third parties*», § 86).

⁵⁶ Il riferimento è alla relazione illustrativa del d.d.l. che ha portato all'introduzione dell'art. 615-ter c.p., ove si sottolineava che i sistemi informatici/telematici rappresentano «un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 del codice penale» (cfr. *supra*, nt. 39). Tale argomento, tuttavia, non coglie le intrinseche diversità che contraddistinguono domicilio tradizionale e informatico.

incorsi in alcuna responsabilità ai sensi dell'art. 615-ter c.p.⁵⁷. La persona interessata dal provvedimento è infatti il legittimo titolare dei dispositivi informatici, di cui, essendo in possesso delle relative credenziali di accesso, può fruire liberamente. Le società, i cui dati avrebbero potuto essere contenuti nei dispositivi, non vantano invece alcun potere di ingerenza sul sistema informatico (computer e cellulare), la cui riservatezza esaurisce l'oggettività giuridica del reato⁵⁸ e, pertanto, ne esclude la configurabilità nel caso di specie.

Affrontata la prima questione giuridica di interesse, occorre ora soffermarsi sulla seconda tematica trattata nel provvedimento della *High Court of Justice*.

4. La nozione di giusta causa ai sensi dell'art. 622 c.p.: l'ordine dell'autorità britannica esclude la configurabilità del reato.

La seconda questione con cui il giudice britannico è stato chiamato a confrontarsi riguarda la potenziale configurabilità del reato di cui all'art. 622 c.p. (rivelazione di segreto professionale): il delitto sarebbe derivato dall'accesso (abusivo) al computer e al telefono del debitore convenuto e, dunque, dall'estrazione dei dati ivi asseritamente contenuti, conformemente a quanto richiesto dal *McCloud Order*.

A tacere della sussistenza o meno di un obbligo giuridico di adempiere alla richiesta dell'autorità britannica sulla base del diritto dell'Unione europea⁵⁹, l'interrogativo di maggiore interesse attiene alla possibilità di qualificare il citato *McCloud Order* come giusta causa rilevante ai fini dell'esclusione della penale rilevanza della condotta di rivelazione. La disposizione incriminatrice, infatti, ancora la tipicità del reato all'assenza di giusta causa della rivelazione (ovvero all'impiego della notizia a proprio o altrui profitto), nonché alla possibilità che dalla condotta derivi nocumento.

La formula linguistica riflette nuovamente l'inquadramento dogmatico di cui si è fatto cenno con riferimento all'avverbio "abusivamente", vale a dire la ripartizione tra clausole di illiceità espressa e clausole di illiceità speciale (*supra*, § 3.⁶⁰). Come già osservato in relazione al reato di accesso abusivo a sistema informatico, può ritenersi che la formula di illiceità (qui: "senza giusta causa") abbia una valenza diversa rispetto alla mera assenza di cause di giustificazione. Il perimetro applicativo della giusta causa non andrebbe dunque sovrapposto *tout court* all'insieme delle scriminanti codificate, dovendosi invece riconoscere l'esistenza di ulteriori situazioni atipiche idonee a escludere la penale rilevanza della condotta⁶¹. Clausole di questa natura – ha affermato la Corte costituzionale – «sono destinate a fungere da "valvola di sicurezza" del meccanismo repressivo, evitando che la sanzione penale scatti allorché – anche al di fuori della presenza di vere e proprie cause di giustificazione – l'osservanza del precetto appaia

⁵⁷ §§ 86 ss. del provvedimento.

⁵⁸ La valutazione sarebbe potuta essere eventualmente differente qualora i dati fossero stati a loro volta protetti da misure di sicurezza diverse e ulteriori rispetto a quelle previste per il computer/cellulare, in tal caso manifestandosi la volontà del titolare dei dati di salvaguardarne la riservatezza. Tale ragionamento ipotetico è avanzato anche dal giudice britannico (cfr. § 89). L'eventuale rilevanza penale di questo esempio richiederebbe nondimeno una modifica della fattispecie incriminatrice: sebbene protetti da misure di sicurezza, i dati presenti all'interno del dispositivo non costituirebbero infatti un sistema informatico/telematico rilevante ai fini dell'art. 615-ter c.p. Per alcune osservazioni ulteriori a riguardo si rinvia *infra* § 5.

⁵⁹ Cfr. §§ 107-108 del provvedimento. La questione atteneva alla natura giuridica (vincolante o meno) del *McCloud Order* alla luce del recesso dall'Unione europea esercitato dal Regno Unito ai sensi dell'art. 50 TUE. A tal riguardo, il giudice britannico osserva che l'atto unionale di interesse – il regolamento (UE) n. 1215/2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale – avrebbe dovuto trovare ugualmente applicazione in quanto il procedimento in questione era stato instaurato prima del termine finale del periodo di transizione che avrebbe portato il Regno Unito alla definitiva uscita dall'Unione europea. In particolare, l'art. 67, par. 2 dell'Accordo di recesso recitava quanto segue: «In the United Kingdom, as well as in the Member States in situations involving the United Kingdom, the following acts or provisions shall apply as follows in respect of the recognition and enforcement of judgments, decisions, authentic instruments, court settlements and agreements: (a) Regulation (EU) No 1215/2012 shall apply to the recognition and enforcement of judgments given in legal proceedings instituted before the end of the transition period [...]». Trovando dunque applicazione al caso di specie il menzionato regolamento, ad avviso del giudice il *McCloud Order* integrava la nozione di giusta causa, così escludendo in radice la configurabilità del reato di cui all'art. 622 c.p. Del resto, era stata la stessa difesa del debitore convenuto ad affermare che, se l'ordine fosse stato emesso da una Corte tedesca, allora questo sarebbe stato sicuramente vincolante per via della normativa eurounitaria (avrebbe dunque configurato la giusta causa).

⁶⁰ V. in particolare nt. 29.

⁶¹ MORGANTE (2002), pp. 145 ss. L'Autrice – per sostenere il diverso ambito di applicazione della giusta causa rispetto alle scriminanti codificate – evidenzia come il legislatore abbia deciso di prevedere l'inciso ("senza giusta causa") esclusivamente nei delitti di rivelazione di segreti privati e non, invece, nei reati di rivelazione di segreti di Stato, che rimarrebbero comunque coperti dall'operare delle cause di giustificazione in senso stretto.

concretamente “inesigibile” in ragione, a seconda dei casi, di situazioni ostative a carattere soggettivo od oggettivo, di obblighi di segno contrario, ovvero della necessità di tutelare interessi confliggenti, con rango pari o superiore rispetto a quello protetto dalla norma incriminatrice, in un ragionevole bilanciamento di valori⁶².

La nozione di “giusta causa” – lungi dall’essere circoscritta al perimetro delle cause di giustificazione codificate – riflette allora parametri elastici di matrice etico-sociale, ancor prima che giuridica, la cui sussistenza dovrà essere valutata dal giudice nel caso concreto⁶³. Si farebbe riferimento, in altre parole, a un generico concetto di giustizia da accertare volta per volta⁶⁴.

Ribadito che le clausole di illiceità speciale (qui la giusta causa) svolgono una funzione diversa rispetto alle cause di giustificazione in senso stretto⁶⁵, le motivazioni del provvedimento in analisi, con specifico riguardo alla definizione del concetto di “giusta causa”, riflettono, in maniera per vero poco approfondita, l’orientamento dottrinale c.d. misto (su cui meglio *infra*). Il giudice ha dapprima riconosciuto l’esistenza di un contro-interesse di valore almeno equivalente a quello tutelato dalla norma incriminatrice, in tal modo giustificando la rivelazione del segreto (*id est* i dati riferibili alle società di cui il convenuto era stato amministratore)⁶⁶. In particolare, da un lato veniva in rilievo l’interesse delle parti attoree all’esecuzione del provvedimento di condanna (dunque al pagamento in loro favore da parte del debitore delle somme quantificate nella decisione), dall’altro emergeva l’interesse a che le informazioni presenti sul sistema informatico rimanessero riservate (*ergo* l’interesse alla segretezza tutelato dal reato di cui all’art. 622 c.p.). In secondo luogo, il giudice ha ritenuto che l’azione intrapresa dalle parti attoree – culminata nell’emissione del *McCloud Order* – fosse la più immediata per ottenere l’esecuzione della condanna del debitore al pagamento delle somme⁶⁷.

L’argomentare della *High Court of Justice* merita due notazioni.

La prima, di carattere più generale, attiene alla scelta di prendere in considerazione, ai fini della valutazione della giusta causa, due diversi criteri, così aderendo a quello che è stato già definito come orientamento misto⁶⁸: (i) il rapporto di proporzione tra gli interessi in gioco, che si risolve in un’opera di bilanciamento degli stessi; la giusta causa sussiste qualora il contro-interesse al mantenimento della segretezza abbia valore maggiore o equivalente; (ii) la necessità della rivelazione, che si traduce nell’inevitabilità della condotta per raggiungere lo scopo lecito perseguito dal soggetto attivo. La posizione assunta dal giudice britannico è condivisibile. Fondare la valutazione in punto di giusta causa esclusivamente sulla sussistenza di uno dei due elementi richiamati non pare infatti essere sufficiente. Da un lato, il solo bilanciamento di interessi – criterio di per sé vago e indeterminato – rischierebbe di riversare sul magistrato un accertamento particolarmente complesso, specie se si considera il fatto che di sovente dovrebbero essere ponderati interessi patrimoniali e non patrimoniali⁶⁹. Dall’altro lato,

⁶² Corte cost., 13 gennaio 2004, n. 5, in www.cortecostituzionale.it, su cui GROSSO E. (2004), pp. 97 ss.; nonché CALCAGNO (2004), pp. 839 ss. I concetti elaborati dalla Corte costituzionale sono stati più di recente richiamati dalla Corte di cassazione (Cass., sez. V, 7 gennaio 2021, n. 318, in *Onelegale*), che, nel caso di specie, ha riconosciuto la sussistenza della giusta causa nella condotta di rivelazione posta in essere da un ginecologo che, nel rilasciare un certificato medico, aveva comunicato a una propria paziente circostanze riservate riguardanti le condizioni sessuali e le capacità procreative del marito.

⁶³ Già PEDRAZZI (1980), p. 250. Si veda, inoltre, MANCA (2014), p. 513.

⁶⁴ Nella prassi, Cass., sez. V, 7 gennaio 2021, n. 318, cit.; Cass., sez. V, 15 dicembre 2014, n. 52075, Rv. 263226; Cass., sez. V, 1° ottobre 1997, n. 8838, in *Onelegale*, con nota di GALLUCCI (1998), p. 1380; LARIZZA (1998), pp. 2361 ss. A tal proposito, la già menzionata Corte costituzionale (Corte cost., sent. n. 5/2004, cit.) aveva osservato che il «carattere “elastico” della clausola si connette, nella valutazione legislativa, alla impossibilità pratica di elencare analiticamente tutte le situazioni astrattamente idonee a “giustificare” l’inosservanza del precetto. Una simile elencazione sconterebbe immancabilmente – a fronte della varietà delle contingenze di vita e della complessità delle interferenze dei sistemi normativi – il rischio di lacune: lacune che, peraltro, tornerebbero non a vantaggio, ma a danno del reo, posto che la clausola in parola assolve al ruolo, negativo, di escludere la punibilità di condotte per il resto corrispondenti al tipo legale».

⁶⁵ In argomento, nuovamente MORGANTE (2002), pp. 134 ss.

⁶⁶ § 109 del provvedimento: «*Thirdly, there is also a very strong argument that this is a situation where a reasonable balancing of values results [...] being permitted to comply with the order of Master McCloud, and without committing any offence. There has been a lawful order of the English court in a case which has long been dealt with in England, and where jurisdiction clearly exists. There is an obvious need [...] to enforce its existing judgment, and the purpose of the order is to assist in enabling it to do so.*»

⁶⁷ § 110 del provvedimento. In particolare, il giudice, nel rispondere alle osservazioni avanzate dalla difesa del convenuto, afferma: «*It is by no means clear to me that there are any such easy routes. I was not persuaded as to the ease of [...] being able to obtain equivalent relief by making an application to join the companies for the purposes of obtaining disclosure, and the precise method by which such an application could successfully be made was not spelt out in the submissions on [...]. It seems to me that a far more straightforward and easy route is the one which [...] has initiated via the orders made [...] in these proceedings, culminating in the order of Master McCloud.*»

⁶⁸ Per una panoramica dei vari orientamenti, LOTTINI (2022), pp. 6777 ss.

⁶⁹ È questo il criterio che sembra essere utilizzato da Cass., sez. V, 1° ottobre 1997, n. 8838, cit. Nel caso di specie, la Suprema Corte ha annullato senza rinvio la sentenza di condanna dell’imputato che, dopo aver preso cognizione della corrispondenza bancaria indirizzata alla moglie, aveva prodotto la documentazione nel procedimento di separazione.

il solo criterio della necessità (*rectius* inevitabilità del mezzo) potrebbe portare a far prevalere interessi di portata concretamente meno rilevante rispetto alla segretezza (sebbene tutelati dall'ordinamento)⁷⁰. Maggiormente convincente, allora, è la combinazione di entrambi gli elementi: rapporto di proporzione e necessità. Già autorevole dottrina sottolineava a riguardo come la rivelazione possa dirsi legittimata dalla presenza di una giusta causa qualora «necessaria a salvaguardare l'integrità di interessi preminenti, alla stregua dei valori dominanti nella coscienza sociale, rispetto all'interesse alla conservazione del segreto»⁷¹. Occorre da ultimo precisare che siffatta valutazione deve essere necessariamente effettuata in concreto, altrimenti ingenerandosi la possibilità che, ad esempio, interessi di natura strettamente patrimoniale vengano nella maggior parte dei casi giudicati recessivi rispetto ad altri. Il giudice, in altre parole, deve prendere in considerazione le conseguenze che si produrrebbero in capo alle parti come conseguenza della rivelazione o meno del segreto.

La seconda, e conclusiva, notazione guarda più direttamente al ragionamento argomentativo del giudice. Quest'ultimo – pur avendo fatto propri entrambi i criteri di valutazione (bilanciamento di interessi e inevitabilità della rivelazione) – non sembra cogliere sino in fondo il valore del requisito della necessità, che, come osservato, vorrebbe che la rivelazione sia l'unico mezzo a disposizione del soggetto per perseguire il proprio scopo (qui: l'esecuzione della decisione di condanna del debitore). Senza voler scendere nell'analisi degli strumenti giuridico-normativi previsti nell'ordinamento britannico, basti qui evidenziare come il giudice definisca le azioni intraprese dalle parti attoree come la strada più semplice e immediata per conseguire il risultato giudiziario. Non sembra allora esserci un giudizio in termini di inevitabilità del mezzo impiegato – ed è questo l'aspetto criticabile – bensì di mera convenienza processuale⁷².

In definitiva, la struttura argomentativa del provvedimento – sebbene sia decisamente apprezzabile in punto di valutazione di entrambi i criteri sopra accennati (bilanciamento di interessi e necessità) – pare essere parzialmente carente, da un punto di vista motivazionale, nella parte in cui analizza l'elemento della inevitabilità dello strumento che avrebbe portato alla rivelazione del segreto.

5. Osservazioni conclusive.

Il provvedimento emesso dalla *High Court of Justice* è di particolare interesse per l'osservatore italiano. Due le questioni affrontate dal giudice britannico: (i) la configurabilità del reato di accesso abusivo a sistema informatico/telematico qualora all'interno del dispositivo – cui accede il legittimo titolare – siano presenti anche dati riferibili a soggetti terzi; (ii) la riconducibilità dell'ordine emesso dall'autorità britannica (*McCloud Order*) alla categoria della giusta causa di cui all'art. 622 c.p. L'esito decisorio cui si perviene – mancata configurabilità di entrambe le fattispecie incriminatrici – deve essere condiviso.

La seconda questione taglia in maniera trasversale gli argomenti affrontati nel presente lavoro (*supra*, in particolare §§ 3. e 4.). Sia l'art. 615-ter c.p., sia l'art. 622 c.p. sono contraddistinti da clausole di c.d. illiceità speciale, tradotte normativamente con le formule “abusivamente” e “senza giusta causa”. L'aspetto interessante da richiamare in proposito attiene alla funzione svolta da clausole di tal genere nell'economia del reato. Non costituiscono una mera enfaticizzazione dell'antigiuridicità della condotta (*rectius* della non sussistenza di cause di giustificazione in senso stretto), bensì operano sul piano della tipicità dell'illecito penale⁷³. L'assenza di abusività (nell'introduzione o nel mantenimento all'interno del sistema) o, *a contrario*, la presenza di una giusta causa della rivelazione elide l'esistenza del fatto tipico. Le clausole di illiceità speciale – lungi dall'essere circoscritte all'area dell'antigiuridicità – colorano pertanto i confini della tipicità del reato.

⁷⁰ L'orientamento è sostenuto da CRESPI (1952), pp. 129 ss. Più di recente – a commento della già citata Cass., sent. n. 8838/1997 – LARIZZA (1998), p. 2366. In giurisprudenza, il requisito della necessità del mezzo è valorizzato da Cass., sez. V, 9 gennaio 2014, n. 585, consultabile in *Onelegale*. Nel caso di specie, la rivelazione del segreto – avvenuta nell'ambito di un procedimento di separazione coniugale – non è stata considerata necessaria in quanto, ai sensi dell'art. 210 c.p.c., il giudice avrebbe potuto, anche ad istanza di parte, ordinare l'esibizione dei documenti utili ai fini della decisione.

⁷¹ PEDRAZZI (1980), p. 250.

⁷² V. nuovamente § 110 del provvedimento.

⁷³ Come osservato, MORGANTE (2002), pp. 139 ss. riconosce nelle clausole di illiceità speciale una funzione di delimitazione della rilevanza penale della condotta.

Relativamente invece alla configurabilità del delitto di accesso abusivo a sistema informatico/telematico, deve constatarsi che, alla luce del vigente assetto normativo, l'art. 615-ter c.p. tutela la libera ed esclusiva fruizione del sistema informatico/telematico – ergo la sua riservatezza – da parte di chi ha il potere di escludere gli altri dall'accesso o dal successivo mantenimento al suo interno. A nulla rileva, invece, la presenza nello spazio virtuale di dati riferibili a soggetti terzi. La riservatezza di queste informazioni, infatti, non ricade nell'ambito applicativo della disposizione incriminatrice, incentrata, lo si è visto, sulla perimetrazione dell'abusività della condotta in funzione delle prescrizioni di funzionamento del sistema impartite dal relativo titolare (*supra*, §§ 3. ss.). A tal proposito, può essere interessante fare un cenno conclusivo, in una prospettiva *de iure condendo*, alla proposta di riforma elaborata dal gruppo di lavoro dell'AIPDP⁷⁴.

La disposizione incriminatrice oggetto della proposta⁷⁵ deve essere salutata con favore nella parte in cui riformula la condotta tipica quale accesso senza autorizzazione o in eccesso dei suoi limiti: non più, dunque, introduzione o mantenimento abusivo. L'ipotesi di novella normativa si pone così in linea di continuità con quanto già osservato da una parte della giurisprudenza e della dottrina (*supra*, § 3.1.): il disvalore della fattispecie incriminatrice si esaurisce nella violazione delle prescrizioni (*rectius* dell'autorizzazione), impartite dal titolare del sistema, che regolano modalità e condizioni di utilizzo del dispositivo. Tale formulazione sarebbe al contempo coerente con il bene giuridico della riservatezza informatica (*supra*, § 3.2.), declinato in termini di libera fruizione del sistema da parte di chi ha il potere di concedere l'autorizzazione ad accedervi.

Risulta meno convincente, invece, l'idea di espungere dalla norma l'elemento delle misure di sicurezza – che in uno con l'inciso per cui l'accesso può riguardare anche soltanto una parte del sistema – ambisce a coprire quelle situazioni in cui l'*insider* acceda a spazi o aree del sistema informatico non protetti da misure di protezione⁷⁶. Potrebbe essere il caso del dipendente che accede legittimamente al sistema informatico dell'azienda presso cui lavora – avendone ricevuto l'autorizzazione dal proprio superiore – ma, una volta all'interno del sistema, finisce per consultare una parte dello stesso (es. una memoria in *cloud* priva di password), eccedendo i limiti dell'autorizzazione. O, ancora, potrebbe verificarsi una situazione non lontana da quella oggetto della vicenda *de qua*: il soggetto titolare accede legittimamente al proprio sistema, ma si trova poi a navigare in sezioni in cui sono presenti dati confidenziali riferibili a soggetti terzi. Potrebbe arrivare a sostenersi che, sebbene la persona sia titolare del sistema, l'individuo non abbia l'autorizzazione a consultare parti del proprio dispositivo informatico ove sono collocate informazioni di esclusiva appartenenza altrui.

Ebbene, uno scenario di questo genere non convince sino in fondo. Il solo elemento dell'autorizzazione – a meno di non voler confidare nella predisposizione da parte dei titolari dei sistemi informatici di prescrizioni particolarmente dettagliate – non consentirebbe di distinguere agevolmente il comportamento lecito da quello penalmente rilevante. Non sarebbe affatto semplice, in altre parole, valutare se la persona, una volta entrata all'interno del sistema informatico, abbia o meno ecceduto i confini dell'autorizzazione. Potrebbe allora essere opportuno preservare l'inciso della necessaria apposizione delle misure di sicurezza, che renderebbe manifesta la volontà del titolare di rendere riservata la fruibilità di una determinata area informatica (che sia il sistema interamente considerato o anche soltanto parte di esso). Si garantirebbe in tal modo una maggiore precisione della nuova ipotetica fattispecie incriminatrice.

Bibliografia

A.A.V.v. (2023): *La riforma dei delitti contro la persona. Proposte dei gruppi di lavoro dell'AIPDP* (E-book, DipLap Editore);

⁷⁴ Associazione Italiana dei Professori di Diritto Penale. La relazione, a cura di L. Picotti, R. Flor, I. Salvadori è consultabile sul sito www.aipdp.it. Il contributo è altresì confluito nel volume, consultabile sul medesimo sito, PICOTTI *et al.* (2023), pp. 425 ss. Per un commento alla citata proposta, v. LAMANUZZI (2022).

⁷⁵ «Art. 615-ter c.p. (Accesso non autorizzato ad un sistema informatico): Chiunque accede senza autorizzazione o eccedendo i limiti ad un sistema informatico o ad una sua parte è punito, a querela della persona offesa, con la reclusione fino a tre anni».

⁷⁶ PICOTTI *et al.* (2023), p. 430.

- ALESSANDRI, Alberto (1984): *Riflessi penalistici della innovazione tecnologica* (Milano, Giuffrè);
- ALESSANDRI, Alberto (1990): “Criminalità informatica”, *Rivista trimestrale di diritto penale dell'economia*, pp. 653-661;
- BALSAMO, Antonio (2024): “L’impatto dell’intelligenza artificiale nel settore della giustizia”, *Sistema penale*;
- BASILE, Enrico (2024): “*Crypto assets* e responsabilità penale”, in CONSULICH, Federico (ed.): *Reati in materia bancaria e finanziaria*, in PALAZZO, Francesco, PALIERO, Carlo Enrico, PELISSERO, Marco (eds.): *Trattato teorico-pratico di diritto penale* (Torino, Giappichelli), pp. 451-470;
- BARTOLI, Roberto (2012): “L’accesso abusivo a un sistema informatico (art. 615-ter c.p.) a un bivio ermeneutico teleologicamente orientato”, *Diritto penale contemporaneo – Rivista trimestrale*, 1, pp. 123-127;
- BELLACOSA, Maurizio (2015): “Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle sezioni unite”, *Diritto penale contemporaneo*;
- CALCAGNO, Elisabetta (2004): “I reati dello straniero espulso dopo le modifiche introdotte dalla “legge Bossi Fini””, *Diritto penale e processo*, pp. 839-846;
- CANESCHI, Gaia (2019): “Le nuove indagini tecnologiche e la tutela dei diritti fondamentali. L’esperienza del captatore informatico”, *Diritto penale contemporaneo – Rivista trimestrale*, 2, pp. 419-429;
- CAPPELLINI, Alberto (2022): “I delitti contro la riservatezza informatica”, in CADOPPI, Alberto, CANESTRARI, Stefano, MANNA, Adelmo, PAPA, Michele (eds.): *Diritto penale*, III (Milano, Utet Giuridica), pp. 6719-6751;
- MANCA, Giovanni (2014): “Tutela delle comunicazioni a distanza”, in COCCO, Giovanni e AMBROSETTI, Enrico Mario (eds.): *I reati contro le persone. Trattato breve di diritto penale. Parte speciale* (Padova, Cedam), pp. 506-526;
- CONSULICH, Federico (2018): “Il nastro di *Möbius*. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato”, *Banca borsa e titoli di credito*, pp. 195-234;
- CONSULICH, Federico (2022): “Nella *wunderkammer* del legislatore penale contemporaneo: monete virtuali che causano danni reali”, *Diritto penale e processo*, pp. 153-158;
- CONSULICH, Federico, MAUGERI, Marco, MILIA, Carlo, POLI, Tommaso Nicola, TROVATORE, Gianfranco (2023): “AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?”, *Quaderno giuridico Consob*, 29;
- CONSULICH, Federico (2024): “Intelligenza artificiale e reati finanziari”, in CONSULICH, Federico (ed.): *Reati in materia bancaria e finanziaria*, in PALAZZO, Francesco, PALIERO, Carlo Enrico, PELISSERO, Marco (eds.): *Trattato teorico-pratico di diritto penale* (Torino, Giappichelli), pp. 237-272;
- CORRIAS LUCENTE, Giovanna (1987): “Informatica e diritto penale. Elementi per una comparazione con il diritto statunitense”, *Il diritto dell’informazione e dell’informatica*, pp. 167-201 e pp. 519-553;
- CRESPI, Alberto (1952), *La tutela penale del segreto* (Palermo, Priulla Editore);
- FASANI, Fabio (2017): “Accesso abusivo a sistema informatico: le Sezioni Unite cambiano di nuovo rotta”, *Le Società*, pp. 1393-1407;
- FIANDACA, Giovanni e MUSCO, Enzo (2020): *Diritto penale. Parte speciale. I delitti contro la persona*, II (Bologna, Zanichelli);

- FLOR, Roberto (2012): “Verso una rivalutazione dell’art. 615-ter c.p.?” , *Diritto penale contemporaneo – Rivista trimestrale*, 2, pp. 126-142;
- FLOR, Roberto (2015): “I limiti del principio di territorialità nel *cyberspace*. Rilievi critici alla luce del recente orientamento delle Sezioni Unite”, *Diritto penale e processo*, pp. 1296-1309;
- FLOR, Roberto (2017): “Riservatezza informatica”, *Enciclopedia Treccani, Diritto online*;
- FLOR, Roberto (2018): “La condotta del pubblico ufficiale fra violazione della *voluntas domini*, “abuso” dei profili autorizzativi e “sviamento di potere””, *Diritto penale e processo*, pp. 506-515;
- GALLUCCI, Enrico (1998): “Giusta causa della rivelazione del contenuto della corrispondenza e produzione della corrispondenza violata nel giudizio civile di separazione personale dei coniugi”, *Cassazione penale*, pp. 1380-1381;
- GATTA, Gian Luigi (2022): “Delitti contro l’inviolabilità del domicilio”, in VIGANÒ, Francesco (ed.): *Reati contro la persona*, in PALAZZO, Francesco, PALIERO, Carlo Enrico, PELISSERO, Marco (eds.): *Trattato teorico-pratico di diritto penale* (Torino, Giappichelli), pp. 445-493;
- GIALUZ, Mitja (2019): “Quando la giustizia penale incontra l’intelligenza artificiale: luci e ombre dei *risk assessment tools* tra Stati Uniti ed Europa”, *Diritto penale contemporaneo*;
- GROSSO, Enrico (2004): “«*Ad impossibilia nemo tenetur*»: la Corte detta al giudice rigorosi confini per la configurabilità del reato di ingiustificato trattenimento dello straniero nel territorio dello Stato”, *Giurisprudenza costituzionale*, pp. 97-105;
- LAMANUZZI, Marta (2022): “Accesso abusivo ad un sistema informatico o telematico: prospettive di riforma”, *Archivio penale*;
- LARIZZA, Silvia (1998): “La «giusta causa» quale limite alla libertà e segretezza della corrispondenza”, *Cassazione penale*, pp. 2361-2367;
- LEVI, Nino (1938): “Ancora in tema di illiceità speciale”, in A.A.V.v. (eds.): *Scritti giuridici in memoria di Eduardo Massari* (Napoli, Jovene), pp. 351-371;
- LOTTINI, Riccardo (2022): “Delitti contro l’inviolabilità dei segreti”, in CADOPPI, Alberto, CANESTRARI, Stefano, MANNA, Adelmo, PAPA, Michele (eds.): *Diritto penale*, III (Milano, Utet Giuridica), pp. 6755-6784;
- MANTOVANI, Ferrando (2022): *Diritto penale. Parte speciale. Delitti contro la persona*, I, (Milano, Cedam-Wolters Kluwer);
- MANTOVANI, Marco Orlando (1994): “Brevi note a proposito della nuova legge sulla criminalità informatica”, *Critica del diritto*, 4, pp. 12-22;
- MINO, Antonella (2016): “La tutela penale del “domicilio informatico””, in ROMANO, Bartolomeo (ed.): *Reati contro la persona*, III, in GROSSO, Carlo Federico, PADOVANI, Tullio, PAGLIARO, Antonio (eds.): *Trattato di diritto penale. Parte speciale* (Milano, Giuffrè), pp. 487-505;
- MORGANTE, Gaetana (2002): *L’illiceità speciale nella teoria generale del reato* (Torino, Giappichelli);
- MUCCIARELLI, Francesco (1996): “Commento all’art. 4 della l. 23 dicembre 1993, n. 547 – Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica”, *Legislazione penale*, pp. 98-108;
- PAGELLA, Cecilia (2021): “La Cassazione sulla riconducibilità dei file al concetto di “cosa mobile” oggetto di appropriazione indebita: un caso di analogia in *malam partem*?”, *Sistema penale*;
- PECORELLA, Claudia (2006): *Diritto penale dell’informatica* (Padova, Cedam);

- PECORELLA, Claudia (2021): sub *art. 615-ter c.p.*, in DOLCINI, Emilio e GATTA, Gian Luigi (eds.): *Codice penale commentato* (Milano, Giuffrè), pp. 2051-2071;
- PEDRAZZI, Cesare (1980): “Aspetti penali e processuali del segreto bancario”, in ROMANO, Mario (ed.): *La responsabilità penale degli operatori bancari* (Bologna, Il Mulino), pp. 243-256;
- PICA, Giorgio (1999): *Diritto penale delle tecnologie informatiche* (Torino, Utet);
- PICOTTI, Lorenzo (2000): “Reati informatici”, *Enciclopedia Giuridica*, aggiornamento, VII (Roma, Treccani), pp. 1-36;
- PICOTTI, Lorenzo (2004): “Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati”, in PICOTTI, Lorenzo (ed.): *Il diritto penale dell'informatica all'epoca di internet* (Padova, Cedam), pp. 21-94;
- PICOTTI, Lorenzo (2018): “Profili penali del *cyberlaundering*: le nuove tecniche del riciclaggio”, *Rivista trimestrale di diritto penale dell'economia*, pp. 590-619;
- PICOTTI, Lorenzo, FLOR, Roberto, SALVADORI, Ivan (2023): “Riservatezza e sicurezza informatica, identità digitale”, in AA.Vv. (eds.): *La riforma dei delitti contro la persona. Proposte dei gruppi di lavoro dell'AIPDP* (E-book, DipLap Editor), pp. 423-445;
- PIERGALLINI, Carlo (2015): “I delitti contro la riservatezza informatica (artt. 615-ter, 615-quater, 615-quinquies)”, in PIERGALLINI, Carlo, VIGANÒ, Francesco, VIZZARDI, Matteo, VERRI, Alessandra (eds.): *I delitti contro la persona*, in MARINUCCI, Giorgio e DOLCINI, Emilio (eds.): *Trattato di diritto penale. Parte speciale* (Padova, Cedam-Wolters Kluwer), pp. 769-789;
- PIERGALLINI, Carlo (2024), “Il fatto tipico doloso”, in PALIERO, Carlo Enrico (ed.): *Il sistema penale* (Torino, Giappichelli), pp. 252-284;
- PISANI, Nicola (2020): “La nozione di “cosa mobile” agli effetti penali e i files informatici: il significato letterale come argine all'applicazione analogica delle norme penali”, *Diritto penale e processo*, pp. 651-655;
- PLANTAMURA, Vito (2017): *Domicilio e diritto penale nella società post-industriale* (Pisa, Pisa University Press);
- PULITANÒ, Domenico (1967): “Illiceità espressa e illiceità speciale”, *Rivista italiana di diritto e procedura penale*, pp. 65-124;
- QUATTROCOLO, Serena (2022): “Giustizia penale e intelligenza artificiale: finestre su uno scenario da esplorare”, in PAJNO, Alessandro, DONATI, Filippo, PERRUCCI, Antonio (eds.): *Intelligenza artificiale e diritto: una rivoluzione?* (Bologna, Il Mulino), pp. 533-540;
- ROSSI, Alessandra (1994): “La criminalità informatica: le tipologie di *computer crimes* di cui alla l. 547/93 dirette alla tutela della riservatezza e del segreto”, *Rivista trimestrale di diritto penale dell'economia*, pp. 427-452;
- SALVADORI, Ivan (2023): “I reati contro la riservatezza informatica”, in CADOPPI, Alberto, CANESTRARI, Stefano, MANNA, Adelmo, PAPA, Michele (eds.): *Cybercrime* (Milano, Utet giuridica), pp. 694-762;
- SEMINARA, Sergio (2018): “Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente (art. 615-ter, c. 2, n. 1, c.p.)”, *Rivista di diritto dei media*, 2, pp. 235-250.



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>