ACCESSO ABUSIVO A SISTEMA INFORMATICO E CONSEGUENTE RIVELAZIONE DI SEGRETO PROFESSIONALE

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

di Davide Attanasio

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.

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 impieghi[1]. 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

* I riferimenti del provvedimento sono i seguenti: [2024] EWHC 1263 (Comm), disponibile sulla banca dati *Westlaw*, nonché liberamente accessibile al seguente link https://www.enterprisechambers.com/wp-content/uploads/2024/05/DISCHARGE-APP-JUDGMENT.pdf.

[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.

Editore Associazione "Progetto giustizia penale" | via Festa del Perdono 7, 20122 Milano
c/o Università degli Studi di Milano, Dipartimento di Scienze Giuridiche "Cesare Beccaria"
redazione@sistemapenale.it

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 mercato[3] ovvero in tema di criptovalute che, nella dimensione penalistica, chiamano principalmente in causa fenomeni di matrice riciclatoria[4].

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 criminose[5], quanto dalla prospettiva degli organi investigativi e accertativi[6].

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. 547[7], in recepimento della raccomandazione del Consiglio d'Europa[8]. Il provvedimento legislativo rappresenta uno dei primi e maggiormente significativi interventi di riforma nell'ambito della criminalità informatica[9], finalizzato, come osservato in dottrina[10], a fronteggiare il fenomeno dei c.d. *hackers*. L'art. 4, in particolare, ha aggiunto nella sezione del codice penale riservata all'inviolabilità del domicilio un pacchetto di tre fattispecie

---

[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.

incriminatrici[11], tutte costruite attorno alla tutela del sistema informatico o telematico da potenziali interferenze abusive ed eventualmente pregiudizievoli per la riservatezza dei dati in esso contenuti[12]. 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 3[13].

Il presente lavoro affronta l'argomento accennato nella prospettiva di un provvedimento emesso dalla *High Court of Justice*[14], trovatasi 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 lavorative[15]. Per quanto di interesse – e come meglio si descriverà *infra* (§ 2.) – il convenuto si opponeva alla richiesta emessa dall'autorità britannica[16] 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 richiamate[17]. 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.

---

[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.

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 decisione[18]. 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 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 italiano[20] – il giudice britannico si confronta con le fattispecie

---

[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).

[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

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 professionale[22]. Il dialogo tra le difese – le cui tesi non paiono per vero totalmente inconciliabili (*infra*, § 4.), differentemente 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 verificazione del nocumento, 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

---

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.

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 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 telematico[23] e di misure di sicurezza poste a protezione del dispositivo[24], la questione realmente problematica, per quanto qui di interesse, attiene alla delimitazione della condotta tipica.

---

[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'aggiramento 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 aggiramento), 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.

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* accesso[25]), 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 autorizzazione[26].

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 della condotta, non aggiungendo alcunché alla portata della fattispecie incriminatrice[27]. 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 speciale[28].

---

[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».

[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

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 lecito[29]. 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 comportamento[30].

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-penali che stabiliscono le condizioni di accesso al sistema informatico/telematico[31]. 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.

---

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 extrapenali».

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 verificazione della condotta[32]. 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 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 legittimità[33], su profili di carattere soggettivo.

In particolare, il contenuto oggettivo dell'abusività è perimetrato in funzione delle prescrizioni[34] 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'apposizione delle misure di sicurezza[35] – 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]).

---

[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.

[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.

La lettura soggettivistica della fattispecie incriminatrice[37] – 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 passato[40].

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, incentrate sull'individuazione del bene giuridico tutelato.

---

[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*».

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

Prima di scendere nel merito del principale argomento approfondito dal giudice britannico[41] – 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 contenute[42]. 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 sfaccettature[46]. A tacere di opinioni

---

[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).

minoritarie[47], il panorama è conteso principalmente da due orientamenti[48], che emergono anche dalla lettura del provvedimento in analisi[49].

Un primo orientamento – accolto in maniera pressoché costante in giurisprudenza[50] – 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].

Un secondo orientamento, accolto perlopiù in dottrina[52], 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 integrato[53].

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 sistema[54] – 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.

---

[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.

[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.

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 tradizionale[55]. 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 teleologica[56] – 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

---

[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.

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 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 reato[58] 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 europea[59],

---

[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

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, àncora 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 condotta[61]. 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 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 valori»[62].

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 concreto[63]. Si farebbe riferimento, in altre parole, a un generico concetto di giustizia da accertare volta per volta[64].

---

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.

[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

Ribadito che le clausole di illiceità speciale (qui la giusta causa) svolgono una funzione diversa rispetto alle cause di giustificazione in senso stretto[65], 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 somme[67].

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 misto[68]: (*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

---

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.

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 patrimoniali[69]. Dall'altro lato, 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 processuale[72].

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.

---

[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.

[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.

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 enfatizzazione dell'antigiuridicità della condotta (*rectius* della non sussistenza di cause di giustificazione in senso stretto), bensì operano sul piano della tipicità dell'illecito penale[73]. 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.

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'AIPDP[74].

La disposizione incriminatrice oggetto della proposta[75] deve essere salutata con favore nella parte in cui riformula la condotta tipica quale accesso senza autorizzazione

---

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

[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

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 protezione[76]. 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.

---

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.

Bibliografia

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

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.