CONVEGNI

MARTA LAMANUZZI

Accesso abusivo ad un sistema informatico o telematico: prospettive di riforma[1]

Premesso un inquadramento generale della fattispecie di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-*ter* c.p. e delle principali controversie giurisprudenziali e dottrinali che l'hanno interessata, il contributo mira a esaminare e commentare la riformulazione della norma suggerita dal VII Gruppo di lavoro dell'AIPDP nell'ambito della proposta di riforma dei reati contro la persona. L'evoluzione della fenomenologia degli accessi non autorizzati stimola, in conclusione, una riflessione sull'individuazione dell'interesse tutelato e sulla modulazione della risposta sanzionatoria alla luce del principio di proporzione.

Abusive access to an IT or telematic system: perspectives on reform

After a general insight into the crime of abusive access to an IT or telematic system (article 615-ter of the Criminal Code) and of the main jurisprudential and doctrinal disputes to which it gave rise, the paper aims at examining and commenting on the revision of the rule suggested by the VII AIPDP Working Group in the context of the proposal to reform the provisions dealing with offences against individuals. Finally, the evolution of the phenomenology of unauthorized accesses stimulates a reflection on the identification of the protected interest and on the modulation of the sanctioning response in light of the principle of proportionality.

1. *L'influenza della rivoluzione tecnologica sul formante legislativo.* Il rapporto fra rivoluzione tecnologica e politica criminale si articola in più direzioni. Da una parte, i *mass media* influenzano notevolmente la percezione sociale del crimine, in quanto «il sistema mediatico funge da suscitatore del consenso

[1] Il contributo trae spunto dalla relazione tenuta in occasione del Seminario AIPDP del VII Gruppo di lavoro sulla riforma dei reati contro la persona dal titolo "*Reati contro l'inviolabilità del domicilio, la tutela della vita privata e dei segreti, la libertà e la personalità informatica*", tenutosi a Verona il 10 settembre 2021, e sarà pubblicato anche nella relativa raccolta di atti all'interno della Collana DIPLAP (*www.redazionediplap.wixsite.com*).

sociale (...) e da collettore dei bisogni di pena»[2]. Dall'altra, l'avvento degli strumenti informatici, della rete e dei *social network* ha dato luogo a un'ampia fenomenologia di offese ai beni giuridici tradizionali così come a interessi di nuova emersione[3]. Con riferimento a questo secondo profilo, vi è

[2] AMISANO, *Media e diritto: circolo virtuoso o vizioso?*, in *Revista Brasileira de Estudos Políticos*, 2019, 415. In particolare «il filtro che i media operano sulla realtà, attraverso la selezione di determinati aspetti del crimine su cui vengono espressi giudizi di valore, concorre a formare l'idea dei comportamenti che devono costituire reato e di come lo Stato si adoperi per combattere la delinquenza» ed è «inevitabile che questo crei pressioni sullo Stato, perché ingenera nei consociati fiducia o sfiducia sulle capacità della giustizia penale di fronteggiare il crimine, dando ai cittadini quel tanto cercato senso di sicurezza». Peraltro – si precisa – «l'influenza mediatica sulle scelte del legislatore ha un significato ancora più pregnante: la questione da risolvere non è come i media distorcano la realtà, ma piuttosto come essi la costruiscano». *Ivi*, 406, rinviando a LUHMANN, *La realtà dei mass media*, Milano, 2000 (Cfr. anche *La televisione del crimine*, a cura di Forti, Bertolino, Milano, 2005. A parere dell'Autrice, nulla osta a che gli interessi meritevoli di tutela penale emergano o vengano enfatizzati anche dai mezzi di comunicazione, «quel che desta perplessità è l'azione del legislatore, priva di coordinamento e di programmazione e basata – ormai sempre – sulle continue emergenze». Viene così messo in luce come «da ormai molto tempo il legislatore non abbia una visione a lungo raggio – o anche solo a medio raggio – dell'intervento normativo in materia penale. Le leggi sono emanate sull'onda emotiva dell'una piuttosto che dell'altra emergenza. Il che ha portato autorevole dottrina a parlare di emergenza continua. Il legislatore, passando da emergenza a emergenza, crea norme contingenti, senza adeguata pianificazione prospettica e molto spesso senza adeguato e necessario coordinamento. Come è chiaro, se l'emergenza diventa continua, perde le caratteristiche che la contraddistinguono per diventare normalità. Quel che resta è una farneticante proliferazione normativa che non si basa su un progetto, un'idea di fondo, ma resta legata alle contingenze temporanee. È quel che accade quando le risposte del legislatore alle necessità sociali sono non adattative, cioè viscerali: la giustizia diventa più soggetta a influenze esterne e agli umori sociali. In questo modo il decisionismo diventa populista, preoccupandosi più della risposta a breve termine del consenso popolare che delle soluzioni più efficaci benché impopolari. Arrivando al paradosso che si perde la politica legislativa a fronte di una legislazione politica». *Ivi*, 413. Si veda anche PALIERO, *Il Mercato della Penalità. Bisogno e Meritevolezza di pena nel* rationale *della punitività,* Torino, 2021, ove, con riferimento alla criminalizzazione in astratto si sottolinea come non si possano trascurare «la fisionomia e le dinamiche del consumatore» dei «prodotti deontici [le fattispecie di reato], a sua volta propositore di istanze di produzione dosate sui suoi bisogni, reali o soltanto percepiti». In tale ricostruzione il «modello *ideale*» è rappresentato dalla «perfetta coincidenza» fra «istanze emotivo-sociali e razionali-istituzionali». *Ivi*, 100.

[3] Si è affermato a tal proposito che alla «rivoluzione cibernetica» va riconosciuta «un'importanza strutturale o, se si preferisce, strategica per l'evoluzione del diritto, (...) in quanto rappresenta la frontiera più avanzata dell'innovazione e del cambiamento nell'odierna società globalizzata». PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in *Cybercrime*, a cura di Cadoppi, Milano, 2019, 36. Ancora, la disciplina giuridica della rete «si pone come una sorta di banco di prova per il diritto, che si confronta con l'ineludibile necessità di adottare istituti adeguati alle peculiarità di un fenomeno ormai non più nuovo, ma dalla sconvolgente portata eversiva». MENSI, FALLETTA, *Il diritto del Web*, II ed.,

chi ha osservato come «la rivoluzione tecnologica a cui stiamo assistendo abbia influito – talvolta in maniera eclatante» – «sulle categorie concettuali che si trovano alla base della scienza penalistica», «dotando i concetti basilari del diritto penale di una dimensione ulteriore e forse ancora non del tutto compresa ed esplorata»[4]. Il nuovo habitat cibernetico in cui si sviluppano i rapporti sociali ed economici costituisce quindi «un importante banco di prova per il penalista che deve confrontare il proprio "sapere giuridico" con il "sapere empirico", inteso sia quale "sapere tecnico", indispensabile per cogliere e penetrare le situazioni, le procedure e le condizioni che sono oggetto o risultato dell'automazione informatica, che quale "sapere sociale", in grado di considerare l'incidenza delle applicazioni predette sui comportamenti lesivi e dunque sui *modelli* (o tipi) dei fatti criminosi emergenti, richiedenti un corrispondente adeguamento delle risposte normative e sanzionatorie necessarie a garantire corretti rapporti fra soggetti (ed enti) nel nuovo contesto»[5].

In particolare, con l'evoluzione delle tecnologie digitali, il legislatore si è trovato a fronteggiare almeno due nuove sfide[6]. La prima è stata quella di individuare e qualificare le condotte offensive aventi come oggetto materiale i dispositivi informatici, le reti e i dati in essi contenuti; la seconda è stata quella

---

Padova, 2018, 61.

[4] AMATO MANGIAMELI, SARACENI, *Reati informatici. Elementi di teoria generale e principali figure criminose*, Torino, 2019, X. Continuano gli Autori: «la rivoluzione digitale sembrerebbe aver comprovato l'antica profezia marxiana in base alla quale ogni cosa sarebbe divenuta un giorno volatile. Posto di fronte a una simile *liquefazione*, lo studioso del diritto – e in particolar modo del diritto penale – non può non avvertire un senso di spaesamento e di vertigine. Anche la ricchezza digitale richiede di essere tutelata: il traffico planetario di dati, informazioni e programmi che transitano senza sosta sul *world wide web* necessita di essere organizzato e disciplinato». *Ivi*, XI.

[5] PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in *Tutela penale della persona e nuove tecnologie*, a cura di Picotti, Padova, 2013, 33-34. «Le nuove tecnologie» – viene ancora sottolineato – «determinano essenziali modificazioni e del tutto inedite possibilità d'intervento nella sfera dei diritti e interessi della persona, cambiando i modi di comportamento e i tipi di rapporto in cui essa viene coinvolta (...), per cui si delineano, da un lato, nuove e più specifiche esigenze di tutela e, dall'altro, originali ambiti di autonomia e di libertà della persona da salvaguardare rispetto all'intervento penale». *Ivi*, 32.

[6] «Le moderne tecnologie» hanno, in una certa misura, «messo in crisi» il diritto penale classico ponendolo di fronte alla «necessità di dare una risposta adeguata alle sfide della modernità». In questi termini PLANTAMURA, *Moderne tecnologie, riservatezza e sistema penale: quali equilibri?*, in *Dir. inform.*, 2006, 417.

di intercettare le nuove modalità di condotta, informatiche o telematiche, attraverso le quali hanno iniziato a manifestarsi i reati tradizionali. Si potrebbe distinguere, in tal senso, fra reati informatici "in senso stretto", vale a dire «fattispecie legali che presentano, sul piano della definizione normativa, elementi di tipizzazione descrittivi di modalità, oggetti, attività, specificamente caratterizzati dalla o frutto della tecnologia informatica, vale a dire relativi o connessi a procedimenti di elaborazione automatizzata di dati secondo un programma, come sono per esempio l'accesso abusivo a un sistema informatico (art. 615-*ter* c.p.) o la frode informatica (art. 640-*ter* c.p.)», e reati informatici "in senso lato", ossia «tutte quelle fattispecie che pur non presentando elementi di tipicità del fatto così caratterizzati sul piano tecnico, tuttavia possono includere, nei casi concreti, le predette modalità, attività, oggetti, per l'ampiezza o elasticità dei requisiti costitutivi richiesti dal legislatore, suscettibili d'interpretazione e applicazione evolutiva»[7].

A partire dagli anni Ottanta in diversi Paesi sono intervenute riforme volte a contrastare, spesso con lo strumento della sanzione penale, comportamenti connessi all'impiego delle nuove tecnologie informatiche[8]. In Italia l'atto

[7] PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, cit., 55. Continua l'Autore riferendosi anche alla «categoria dei *reati cibernetici*», che «comprende ulteriormente tutti quelli che, in generale, si realizzano o si possono realizzare, in tutto o in parte, nel *Cyberspace*, e che caratterizzano dunque la dimensione attuale della criminalità informatica, abbracciando entrambe le predette categorie dei reati informatici in senso stretto e in senso lato, sotto il comune requisito della commissione "in rete" di tutto o parte del fatto di reato, bastando che i relativi elementi costitutivi siano *compatibili* con detta realizzazione, almeno in parte, nel *Cyberspace*». Cfr. anche SALVADORI, *I reati contro la riservatezza informatica*, in *Cybercrime*, cit., 657, ove, nell'ambito del diritto penale dell'informatica, viene proposta la distinzione fra reati commessi a danno di strumenti informatici (cd. *computer crime*) e reati commessi per mezzo di strumenti informatici (cd. *cybercrime*), e AMATO MANGIAMELI, SARACENI, *Reati informatici*, cit., XII-XIII, in cui viene fatto riferimento a «reati propriamente informatici», «che esistono perché esistono i computer» («se non esistessero gli elaboratori elettronici, non sarebbe infatti concepibile la diffusione di virus informatici o il possesso abusivo di codici d'accesso») e a «reati *lato sensu* informatici», «che hanno guadagnato una specifica e perniciosa diffusione a causa della rivoluzione digitale, pur aggredendo ben più antichi beni giuridici – come, ad esempio, il patrimonio, la personalità o la riservatezza».

[8] *Ex plurimis*: in Danimarca legge n. 229 del 1985; in Norvegia legge n. 54 del 1987; in Austria legge n. 605 del 1987; in Grecia legge n. 1805 del 1988; in Gran Bretagna *Computer Misure Act* del 1990; negli Stati Uniti *Counterfeit Access Device and Computer Fraud and Abuse* del 1984, poi sostituita dal *Computer Fraud and Abuse Act* del 1986.

normativo cui viene affidato il più significativo adeguamento della legislazione penale al progresso tecnologico è la legge del 23 dicembre 1993, n. 547, recante "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica". Due i principali motori della riforma. Da un lato, occorreva scongiurare la violazione del principio di tassatività in cui rischiavano di incorrere i giudici nel tentativo di applicare le fattispecie esistenti alla nuova realtà digitale[9]. Dall'altro, numerose erano le spinte sovranazionali alla modernizzazione dell'apparato normativo. In particolare, ha svolto un ruolo chiave la "Raccomandazione sulla criminalità informatica", adottata dal Comitato dei Ministri del Consiglio d'Europa il 13 settembre 1989, che, a sua volta, rinviava al "Rapporto sulla criminalità informatica", in cui le «forme di abuso dell'informatica» venivano distinte in due categorie: quelle che gli Stati erano *invitati* a reprimere con la sanzione penale e quelle la cui repressione penale era *lasciata alla discrezionalità* dei legislatori nazionali[10].

Quanto alle modalità della riforma, il legislatore italiano ha introdotto nuove fattispecie, per lo più modellate su figure criminose "tradizionali" (si pensi proprio all'accesso abusivo a sistema informatico o telematico, che è "costruito" sull'attigua fattispecie di violazione di domicilio), e aggiornato ipotesi di reato già presenti affinché potessero trovare applicazione alla nuova casistica. Se la decisione di non ricorrere alla legislazione speciale, intervenendo sul

[9] In dottrina è stato messo in rilievo come «i tentativi di applicazione del tradizionale impianto normativo di parte speciale su condotte di accesso abusivo a sistema informatico – ad esempio, attraverso il ricorso al reato di violazione di domicilio, di sostituzione di persona e di intercettazione abusiva di comunicazioni telefoniche e telegrafiche – sono risultati per lo più inefficienti e potenzialmente lesivi del principio di stretta legalità, stante la diversa materialità del bene giuridico protetto e del mezzo di commissione del reato». BUSSOLATI, *Accesso abusivo a un sistema informatico o telematico ex art. 615*-ter *c.p.: il nodo dell'abusività*, in *Studium iuris*, 2018, 429.

[10] Raccomandazione e Rapporto sono liberamente fruibili su *www.oas.org/juridico/english/89-9&final%20report.pdf.* Fra i fatti contemplati nella "lista minima": la frode informatica, il falso informatico, il danneggiamento dei dati o programmi informatici, il sabotaggio informatico, l'accesso non autorizzato a sistema informatico, l'intercettazione non autorizzata, la riproduzione non autorizzata di un programma informatico protetto e la riproduzione non autorizzata di una topografia. Fra i fatti previsti nella "lista facoltativa": l'alterazione dei dati o dei programmi informatici, lo spionaggio informatico, l'utilizzazione non autorizzata di un elaboratore, l'utilizzazione non autorizzata di un programma informatico protetto.

codice penale, è stata salutata con favore, maggiori perplessità hanno suscitato la scelta di non riservare ai reati informatici "in senso stretto" un titolo *ad hoc*[11] (idea che ritorna, come si vedrà, nelle più recenti proposte di riforma), l'appiattimento delle nuove fattispecie su beni giuridici tradizionali – o su oggetti di tutela forzatamente modellati su detti beni (che avrebbero potuto invece cedere il passo a *nuovi* beni giuridici scaturiti dall'evoluzione tecnologica[12]) – e alcune soluzioni lessicali palesemente inficiate da deficit di conoscenza empirica dei fenomeni da disciplinare (emblematico l'impiego del verbo "introdursi"[13] all'art. 615-*ter* c.p., tecnicamente più appropriato a indicare l'accesso a un luogo fisico che non a un sistema informatico)[14].

2. *L'art. 615-*ter *c.p. quale «fulcro criminologico» dei reati informatici*. La fattispecie di accesso abusivo a un sistema informatico o telematico (art. 615-*ter*

[11] Così MILITELLO, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. econ.*, 1992, 364 ss. Critico in merito anche BUSSOLATI, *Accesso abusivo a un sistema informatico o telematico*, cit., 429-430, il quale sottolinea il rischio, sotteso a tale scelta legislativa, di perdere o quanto meno rendere di difficile comprensione «l'unicità del carattere informatico che tali figure esprimono, a favore invece di una valutazione analogica che benché seducente mal si attaglia alle condotte criminose commesse per mezzo e nei confronti di nuove tecnologie, data anche la costante evoluzione tecnologica». Dello stesso avviso Salvadori (SALVADORI, *I reati contro la riservatezza informatica*, cit., 658), il quale osserva come il legislatore abbia così «rinunciato a cogliere le specificità della criminalità informatica, che incide su beni giuridici, in tutto o in parte, nuovi, non avvedendosi delle significative ricadute che i reati informatici hanno sul piano dogmatico (in relazione al concetto di azione e di evento, al concorso di persone nel reato, al momento consumativo, al *locus commissi delicti*, ecc.)».

[12] In dottrina si è parlato di nuovi "beni informatici", quali strumenti attraverso i quali ormai di frequente il soggetto «esplica la propria personalità e le proprie attività». PIERGALLINI, *I delitti contro la riservatezza informatica (artt. 615-*ter*, 615-*quater*, 615-*quinquies), in PIERGALLINI, VIGANÒ, VIZZARDI, VERRI, *I delitti contro la persona. Libertà personale, sessuale e morale, domicilio e segreti*, in *Trattato di diritto penale. Parte speciale*, diretto da Marinucci, Dolcini, Padova, 2015, Vol. X, 770-771.

[13] Sul punto si veda SALVADORI, *I reati contro la riservatezza informatica*, cit., 667.

[14] Al legislatore è stato rimproverato di essere incorso in un duplice errore: «aver, da un lato, trascurato gli effetti erosivi, per la determinatezza dei concetti tradizionali, della loro estensione a ipotesi del tutto eterogenee, che hanno in comune solo un'analoga funzione, mentre del tutto distinti restano gli specifici elementi costitutivi, alla cui stregua si decide della tipicità dei "nuovi" fatti incriminati; e, dall'altro, aver sottovalutato il profondo condizionamento che tale diversità contenutistica degli "oggetti materiali" delle condotte esercita sulla stessa struttura o modalità esecutiva di queste, fino al punto da porne in discussione, in molti casi, la concreta compatibilità o configurabilità logico-giuridica». PICOTTI, *Commento all'art. 5 della legge n. 547 del 1993*, in *Leg. pen.*, 1996, 109.

c.p.) è stata definita «il fulcro criminologico» dei reati informatici, in quanto si pone «come prodromo per l'eventuale commissione di reati contro l'integrità o la riservatezza dei dati»[15].

La norma sanziona chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo (*ius excludendi alios*). L'"introduzione" può avvenire con qualunque mezzo, sia avendo diretto contatto con il dispositivo elettronico (ad esempio il pc) sia "da remoto", purché si tratti di un sistema provvisto di qualche misura di sicurezza contro gli accessi indesiderati.

«L'espressione "sistema informatico"» – ha precisato la giurisprudenza di legittimità – rimanda a «una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche (...) caratterizzate dalla registrazione (o "memorizzazione"), per mezzo di impulsi elettronici, su supporti adeguati, di dati (...): tali "dati", elaborati automaticamente dalla macchina, generano le informazioni costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di attribuire un particolare significato per l'utente»[16]. Ancora, in dottrina, il sistema informatico viene definito, nel suo contenuto minimo, come «il complesso formato da un *elaboratore elettronico di dati* e dalle periferiche alle quali è connesso»[17]. Il termine "sistema telema-

[15] BUSSOLATI, *Accesso abusivo a un sistema informatico o telematico*, cit., 428. Il già citato Rapporto cui rinvia la "Raccomandazione sulla criminalità informatica" del 1989 invitava i legislatori nazionali a prevedere, fra le altre, una norma che incriminasse l'«accesso non autorizzato» a un sistema informatico, al fine di garantire «in prima battuta, la sicurezza del sistema informatico e l'inviolabilità del domicilio informatico» e, d'altra parte, assicurare «una protezione, in via anticipata e indiretta, contro i rischi di manipolazioni informatiche, di danneggiamento dei dati e di spionaggio informatico».

[16] Cass., Sez. VI, 4 ottobre 1999, Piersanti, in *Dir. inform.*, 2001, 485.

[17] PLANTAMURA, *Domicilio e diritto penale nella società post-industriale*, Pisa, 2017, 200. Ancora – si è specificato in dottrina – «per sistema informatico, si intende il complesso degli elementi fisici e logici, che compongono un apparato di elaborazione automatizzato: dunque, tra gli altri, l'*hardware* (integrato da componenti fisici, magnetici, elettrici) e il *software* (integrato dai programmi, procedure e regole di comportamento)». «Il sistema telematico», invece, «è 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. La telematica vede, dunque, convergere la telecomunicazione, vale a dire la comunicazione a distanza, che elimina ostacoli di natura fisica, e l'informatica, cioè l'elaborazione

tico" indicherebbe invece ogni forma di telecomunicazione tra sistemi informatici e implicherebbe come tale il coinvolgimento di «almeno due apparecchi (...) in comunicazione tra loro per *la trasmissione a distanza dei dati*»[18].
Il sistema deve essere protetto da misure di sicurezza, sebbene non ne sia richiesta né la violazione da parte del soggetto agente né tanto meno l'adeguatezza nel prevenire gli accessi indesiderati. Infatti, come evidenziato dai primi commentatori, «la misura di sicurezza di cui all'art. 615-*ter* c.p. deve essere considerata un elemento eminentemente *semiotico* che non impone all'interprete alcun giudizio di idoneità in concreto»[19]. Secondo parte della dottrina, si tratterebbe di una previsione volta a "responsabilizzare la vittima" subordinando la tutela del sistema al suo "attivarsi" dotandolo di protezioni[20]; secondo altro orientamento, la presenza di misure di sicurezza sarebbe necessaria al fine di delimitare il sistema informatico e telematico, che, a differenza del domicilio, non è "intuitivamente privato"[21].
"Introdursi" in un sistema informatico o telematico ai sensi dell'art. 615-*ter* c.p. consiste nell'ottenere l'accesso alla memoria interna del sistema, mettendosi così nella condizione di poter richiamare i dati e i programmi che vi so-

---

elettronica dei dati. In definitiva, il sistema telematico è un sistema integrato, capace di gestire dati, voci, testi e immagini». PIERGALLINI, *I delitti contro la riservatezza informatica*, cit., 778-779.

[18] PLANTAMURA, *Domicilio e diritto penale*, cit., 200.

[19] AMATO MANGIAMELI, SARACENI, *Reati informatici*, cit., 64.

[20] MANTOVANI, *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Crit. dir.*, 1994, IV, 20; PICOTTI, voce *Reati informatici*, in *Enciclopedia giuridica Treccani*, *Aggiornamento*, Roma, 2000, 22; PECORELLA, *Sub art. 615*-ter *c.p.*, in *Codice penale commentato*, diretto da Dolcini, Gatta, III, Milano, 2021, 2055.

[21] SEMINARA, *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.)*, in *MediaLaws*, 2018, 2, 242. Con le parole dell'Autore: «alle misure di sicurezza viene attribuita la funzione di manifestare all'esterno quello *ius excludendi* che è implicito nel domicilio fisico e che, soprattutto nel mondo della rete, non caratterizza necessariamente ogni sistema: è pertanto indifferente che tali misure siano adeguate od obsolete, facilmente o difficilmente aggirabili, poiché la loro rilevanza si esaurisce in una valenza sintomatica, mirata appunto ad assicurare l'equivalenza tra domicilio reale e informatico». Così anche PLANTAMURA, *Domicilio e diritto penale*, cit., 191 ss. Vi è, ancora, chi ritiene che si tratti di una «scelta politico criminale che, da un lato, mira alla responsabilizzazione del titolare del sistema, anche solo al fine di rendere manifesta la sua volontà di escludere soggetti non autorizzati e, dall'altro lato, pone al centro la violazione della *voluntas domini*, che proprio nella previsione dell'elemento obiettivo della presenza di misure protettive trova manifestazione». FLOR, *La condotta del pubblico ufficiale fra violazione della* voluntas domini, *"abuso" dei profili autorizzativi e "sviamento di potere"*, in *Dir. pen. proc.*, 2018, 514.

no contenuti. In particolare, non è sufficiente un qualsiasi "contatto" con un dispositivo, ma occorre che l'agente istauri un "dialogo logico" con il sistema informatico o telematico, nel senso di utilizzare uno o più comandi da cui deve dipendere l'esecuzione, da parte del sistema, di una certa operazione. Così facendo l'agente si pone nelle condizioni di conoscere il contenuto o le risorse del sistema, pur non essendo necessario, ai fini dell'integrazione della fattispecie, né che effettivamente ne prenda conoscenza né che esegua attività di sorta[22].

La norma punisce inoltre chi, dopo aver compiuto un accesso autorizzato o "casuale", si mantiene nel sistema contro la volontà espressa o tacita del titolare. Si pensi al classico esempio del tecnico che, incaricato di verificare il corretto funzionamento di un computer, una volta portato a termine il lavoro, si trattenga ulteriormente nel sistema mettendosi così nelle condizioni di compiere attività che esulano dal compito che gli era stato assegnato e in relazione al quale era stato autorizzato all'accesso. Anche la permanenza deve essere intesa nel senso di mantenimento della connessione logica[23].

Quanto all'avverbio "abusivamente", su cui si tornerà nel prosieguo[24], secondo parte della dottrina, si limita a rimarcare che l'accesso deve avvenire in assenza del consenso del titolare dello *ius excludendi* e di cause di giustificazione che lo facoltizzino o lo impongano, operando come clausola di illiceità espressa[25]; secondo altro orientamento, si tratterebbe di un elemento del reato, in mancanza del quale verrebbe meno l'antigiuridicità delle condotte, ope-

---

[22] SALVADORI, *I reati contro la riservatezza informatica*, cit., 669. In altri termini, si deve trattare di una «penetrazione di tipo elettronico, telematico o virtuale, e avviene tramite il superamento delle barriere che presidiano l'accesso alla memoria interna del sistema, sì che l'agente guadagna una libertà di movimento all'interno del sistema». Cfr. PIERGALLINI, *I delitti contro la riservatezza informatica*, cit., 774; FASANI, *Accesso abusivo a un sistema informatico: le Sezioni Unite cambiano di nuovo rotta* (nota a Cass., Sez. un., 8 settembre 2017, ud. 18 maggio 2017, Savarese), in *Le Società*, 2017, 1404.

[23] SALVADORI, *I reati contro la riservatezza informatica*, cit., 669.

[24] Vedi *infra* § 4.

[25] Così, ad esempio, MARINUCCI, DOLCINI, GATTA, *Manuale di diritto penale. Parte generale*, X ed., Milano, 2021, 308; PIERGALLINI, *I delitti contro la riservatezza informatica*, cit., 780 (l'Autore fa l'esempio del consulente tecnico che, su indicazione dell'Autorità giudiziaria, accede a un computer sottoposto a sequestro al fine di esaminarne il contenuto); BORRUSO, *La tutela del documento e dei dati*, in BORRUSSO, BUONOMO, CORASANITI, D'AIETTI, *Profili penali dell'informatica*, Milano, 1994, 32; FASANI, *Accesso abusivo a un sistema informatico*, cit., 1405.

rando quale clausola di illiceità speciale[26]. In particolare, la specificazione del carattere abusivo dell'accesso varrebbe ad aggiungere alla contrarietà alle indicazioni espresse o tacite del titolare la mancanza di un titolo autorizzativo[27].
Il dolo richiesto è un dolo generico, che consiste nella volontà di introdursi o di mantenersi nella memoria interna di un elaboratore o in un determinato spazio virtuale in assenza del consenso del titolare dello *ius excludendi* e con la consapevolezza che quest'ultimo li ha presidiati con misure di protezione.

3. *Il dibattito sul bene giuridico tutelato.* Secondo l'impostazione tradizionale, prevalente in giurisprudenza e in linea con la collocazione sistematica della fattispecie e con le indicazioni emerse nel corso dei lavori preparatori, il bene giuridico protetto dall'art. 615-*ter* c.p. coinciderebbe con il *domicilio informatico*, quale «espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli artt. 614 e 615 del codice penale»[28]. Così, secondo un nutrito indirizzo giurisprudenziale, la norma sarebbe stata

[26] Locuzioni quali "ingiustamente", "indebitamente", "arbitrariamente", "abusivamente", ecc. possono avere la valenza di "clausole di illiceità espressa" (o apparente) o di "clausole di illiceità speciale". Nel primo caso si tratta di formule sostanzialmente pleonastiche che non contribuiscono a descrivere il fatto penalmente rilevante ma si limitano a dare *espresso* rilievo alle cause di giustificazione previste dall'ordinamento, in presenza delle quali viene meno l'antigiuridicità del fatto. Nel secondo caso, invece, viene richiesta una nota di illiceità ulteriore, desumibile da una fonte o da una norma diversa da quella incriminatrice, anche non espressamente richiamata da quest'ultima. Cfr. FIANDACA, MUSCO, *Diritto penale. Parte Generale*, VIII ed., Torino, 2019, 205 ss.; PULITANÒ, *Illiceità espressa e illiceità speciale*, in *Riv. it. dir. proc. pen.*, 1967, 65 ss.; RISICATO, *Gli elementi normativi della fattispecie penali. Profili generali e problemi applicativi*, Milano, 2004, 101 ss.

[27] SALVADORI, *I reati contro la riservatezza informatica*, cit., 670-671.

[28] Relazione al Disegno di legge n. 2773 (al Senato il 26 marzo 1993, alla Camera l'11 giugno successivo) presentata dal Ministro di Grazia e Giustizia (Giovanni Conso), 9. Fra i primi commentatori della norma vi è chi ha messo in luce il «valore acquisito dal computer per l'uomo d'oggi quale sorta di propaggine della propria mente e di tutte le conoscenze, i ricordi, i segreti che essa custodisce». BORRUSO, *La tutela del documento e dei dati*, cit., 28. In tal senso, la Cassazione ha da subito precisato come la fattispecie fosse posta a tutela dello «*ius excludendi* del titolare del sistema informatico, quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla propria sfera di pensiero o alla propria attività (lavorativa e non)». Cass., Sez. VI, 4 ottobre 1999, cit. Il "domicilio" informatico, in particolare, andrebbe inteso come *spatium vitae et cogitationis* attraverso cui si estrinseca la personalità umana. GALDIERI, *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997, 147.

introdotta «per assicurare una protezione all'ambiente informatico o telematico che contiene dati personali che devono rimanere riservati e conservati, al riparo da ingerenze e intrusioni altrui, e rappresenta un luogo inviolabile, delimitato da confini virtuali, paragonabile allo spazio privato dove si svolgono le attività domestiche»[29]. Seguendo tale orientamento, il reato in questione deve essere considerato un *reato di danno*, in quanto l'accesso al sistema produce l'immediata lesione dell'interesse all'inviolabilità del domicilio informatico anche nell'ipotesi (sebbene remota) che non vi siano contenuti né dati né programmi, così come la violazione di domicilio ex art. 614 c.p. viene integrata, con piena lesione del bene tutelato, a prescindere dal fatto che il luogo fisico violato contenga mobili od oggetti di sorta[30].

Nonostante la collocazione sistematica della norma, sono andati via via sviluppandosi orientamenti dottrinali critici rispetto a tale impostazione. In particolare, la nozione di domicilio – si è argomentato – non potrebbe essere estesa fino a comprendere le caratteristiche del fenomeno digitale, soprattutto in considerazione dell'emersione di nuovi e cangianti spazi virtuali cui si è assistito con l'evoluzione cibernetica. Si tratta di una nozione che «trasuda fisicità e spazialità, quale proiezione della pace e della tranquillità domestiche (...)» manifestando, così, «una nervatura integralmente naturalistica», laddove invece «la criminalità informatica è, il più delle volte, marcata dall'assenza di fisicità (...)»[31]. In altri termini – si è osservato – «non si tratta, come erronea-

[29] Cass., Sez. un., 24 aprile 2015, (ud. 26 marzo 2015), G.u.p. Roma, in *Riv. pen.*, 2015, 6, 521. Cfr. Cass., Sez. V, 29 maggio 2008, Scimia, in *Cass. pen.*, 2009, 4, 1502 ss.; Cass., Sez. V, 28 ottobre 2015, Bastoni, in *Cass.,* 2017, 1, 144 ss.; Cass., Sez. V, 26 ottobre 2016, Clickpoint s.r.l., in *Guida dir.*, 2017, 22, 41; Cass., Sez. II, 14 gennaio 2019, Ferretti, Appaia, in *Guida dir.*, 2019, 30, 71 ss.; Cass., Sez. II, 29 maggio 2019, F.S., F.A., P.M., in *Riv. dir. ind.*, 2020, 1, II, 98 ss.; Cass., Sez. V, 19 febbraio 2020, L.R., in *Diritto & Giustizia*, 9 giugno 2020.

[30] Precisa Seminara: «al di là di ogni pretesa di identificazione tra il domicilio reale e il domicilio informatico, la norma in esame tutela dunque uno spazio di riservatezza, cioè una sfera di manifestazione della personalità individuale o di autodeterminazione della propria vita privata». Ancora, «la stessa sistemazione del codice penale, ove i reati contro l'inviolabilità del domicilio precedono quelli contro l'inviolabilità dei segreti, conferma che la nozione di riservatezza va intesa come pacifico godimento della propria sfera privata, indipendentemente dal successivo utilizzo dei dati o dei fatti la cui conoscenza viene preclusa a quanti siano privi di una facoltà di accesso». SEMINARA, *Note sul reato di accesso abusivo*, cit., 241-242.

[31] PIERGALLINI, *I delitti contro la riservatezza informatica*, cit., 772. «La condotta umana» – continua

mente ritenuto dal legislatore del 1993, di "luoghi" equiparabili *tout court* alla nozione di domicilio tradizionale, inteso quale spazio fisico di "espansione ideale dell'area di rispetto pertinente al soggetto interessato" (...). Si tratta piuttosto di nuove sfere "virtuali" di libera, esclusiva e immediata disponibilità che, attribuendo ai titolari o ai soggetti legittimati la possibilità di "trattare" con estrema facilità e rapidità un'enorme quantità di dati e di informazioni, permettono di estrinsecare liberamente la propria personalità o di svolgere al loro interno ogni genere di attività (professionale, economica, sociale, culturale, ecc.)»[32].

Sono state così prospettate interpretazioni alternative. Non potendo i sistemi informatici o telematici essere neppure assimilati ai luoghi privati di cui all'art. 614 c.p., effettiva proiezione spaziale della persona, il bene giuridico tutelato dalla norma, secondo un primo filone ermeneutico, andrebbe individuato nell'*indisturbata fruizione del sistema* da parte del gestore, non diversamente da come l'art. 637 c.p., nel reprimere l'ingresso abusivo nel fondo altrui, protegge la proprietà fondiaria da ogni possibile turbativa[33].

Secondo una differente ricostruzione, la fattispecie non andrebbe intesa come reato di danno posto a tutela del domicilio informatico, bensì come *reato di pericolo astratto* volto ad apprestare una tutela anticipata alla *riservatezza*[34] o

---

l'Autore – «si smaterializza: non può reggersi, cioè, senza l'ossatura di centri operativi-decisionali non umani, ma cibernetici, che operano in modo automatizzato, sì che diventa spesso inafferrabile il concetto, sperimentato in sede processuale, di *locus commissi delicti*».

[32] SALVADORI, *I reati contro la riservatezza informatica*, cit., 660-661. Proseguendo nel ragionamento: «in queste nuove sfere di controllo, disponibilità e godimento esclusivo, gli utenti possono non solo raccogliere, organizzare, conservare, elaborare e scambiare informazioni e dati di natura riservata o segreta, nell'accezione tradizionale che tali concetti assumono nel diritto penale, ma anche contenuti informativi di per sé già noti e disponibili, che attraverso *software* e mezzi di trattamento automatizzato acquistano un valore e una utilità del tutto nuovi».

[33] BERGHELLA, BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass.,* 1995, 2333.

[34] PECORELLA, *Sub art. 615*-ter *c.p.*, cit., 2053. *Contra* è stato rilevato come «il diritto penale non si presti a tutelare la riservatezza, la *privacy* o la vita privata; anzi, per l'esattezza, risulta che lo stesso non si presta a tutelare tali beni mediante la previsione di fattispecie *generali* (né, tanto meno, a forma libera). Infatti, se il bene finale che si vuole tutelare è costituito dalla riservatezza della vita privata, allora appare indubitabile, per via dell'indeterminatezza del bene stesso, che una simile tutela può essere efficacemente apprestata con lo strumento penalistico solo in via indiretta, ovvero incriminando la violazione di beni (precisi e determinati) strumentali alla tutela di tale bene finale: il domicilio, ad es. o la segretezza delle conversazioni o delle comunicazioni». PLANTAMURA, *Moderne tecnologie, riservatezza e sistema*

all'*integrità*[35] *dei dati e dei programmi* contenuti nel sistema; impostazione, quest'ultima, che troverebbe conferma nella previsione di un aumento di pena nel caso in cui «dal fatto derivi la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti» (art. 615-*ter*, comma 2, n. 3, c.p.).

Così argomentando, tuttavia, si perviene alla conclusione che oggetto della tutela predisposta attraverso la fattispecie di cui all'art. 615-*ter* c.p. non sia «la dimensione spaziale del sistema informatico, il "contenitore", bensì l'insieme degli elementi ivi contenuti, il suo "contenuto"»[36], pur non comparendo nella norma – si è sottolineato in dottrina – «alcun riferimento al contenuto (dati, programmi, informazioni), ma solo al contenitore (sistema informatico o telematico)» e «la specificazione che debba trattarsi di un contenitore chiuso, protetto da misure di sicurezza, rafforza l'idea che sia proprio il contenitore in sé ad essere protetto appunto in virtù della sua natura di "luogo chiuso"»[37].

Ancora, avverso la soluzione da ultimo richiamata si può obiettare come esistano altre norme che sono poste precipuamente a tutela dei dati (il riferimento è alle norme in tema di protezione dei dati personali) nonché dell'integrità dei sistemi informatici e telematici (si pensi alle fattispecie che reprimono i danneggiamenti informatici).

Ha invece riscosso notevole successo in dottrina la tesi, su cui si tornerà diffusamente nel prosieguo[38], in forza della quale il reato di cui all'art. 615-*ter* c.p. tutelerebbe la *riservatezza informatica*, bene giuridico che andrebbe tenuto distinto sia dalla *privacy* sia dal domicilio, pur essendo legato all'espansione

---

penale, cit., 434. In altri termini «il bene riservatezza risulta, in sé, troppo sfuggente per essere utilizzato dal diritto penale, a meno che non lo si concretizzi in un luogo che diviene oggetto di tutela, nel senso di riservatezza di quel luogo». PLANTAMURA, *Domicilio e diritto penale*, cit., 190.

[35] MANTOVANI, *Brevi note a proposito della nuova legge sulla criminalità informatica*, cit., 18.

[36] CANNATA, COSTALUNGHI, *Accesso abusivo ad un sistema informatico*, in *Trattato di diritto penale. Parte speciale*, a cura di Cadoppi et al., Torino, 2008-2015, 522.

[37] PLANTAMURA, *Domicilio e diritto penale*, cit., 187-188, ove si sostiene che la norma tutelerebbe quindi, ritornando all'impostazione tradizionale, proprio il domicilio informatico «quale spazio, sia ideale che fisico, rispetto al quale il titolare esercita lo *ius excludendi alios*».

[38] Vedi *infra* § 5 e 7.

ideale della riservatezza del titolare dello *ius excludendi alios*[39]. «La riservatezza informatica», in particolare, avrebbe «ad oggetto l'interesse all'esclusività dell'accesso a uno o più spazi informatici, a prescindere dalla natura dei dati e delle informazioni ivi archiviati, nonché alla loro disponibilità rispetto a illegittime interferenze da parte di terzi soggetti»[40].

4. *La* vexata quaestio *dell'abusività dell'accesso e del mantenimento nel sistema informatico o telematico*. In giurisprudenza si sono storicamente alternati due orientamenti in materia di abusività dell'accesso. Secondo il primo[41], il criterio ermeneutico da seguire per stabilire quando un soggetto si introduca o si mantenga abusivamente in un sistema informatico o telematico è di tipo soggettivo, dovendo il giudice verificare se l'agente perseguisse finalità diverse da quelle per cui era autorizzato ad accedere. Contrariamente, stando a un differente filone ermeneutico[42], andrebbe valutata esclusivamente l'oggettiva violazione delle prescrizioni, indicazioni, disposizioni organizzative, prassi che regolavano l'accesso e la permanenza nel sistema informatico o telematico.
Le Sezioni Unite Casani, nel 2011, sono intervenute a dirimere la controversia precisando che la legittimità dell'accesso va valutata sulla base

[39] PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di Internet*, a cura di Picotti, Padova, 2004, 21 ss.; ID., *La tutela penale della persona e le nuove tecnologie dell'informazione*, cit., 60-61; SALVADORI, *I reati contro la riservatezza informatica*, cit., 692, in cui si rimprovera all'orientamento classico, che identifica nel domicilio informatico il bene giuridico tutelato, di attribuire «un valore assorbente alla collocazione topografica, ignorando, però, che quest'ultima è soltanto uno degli strumenti interpretativi per determinare l'effettivo interesse giuridico oggetto di tutela». *Ivi*, 658; FASANI, *Accesso abusivo a un sistema informatico*, cit., 1404.

[40] FLOR, *La condotta del pubblico ufficiale*, cit., 512.

[41] Cass., Sez. V, 7 novembre 2000, Zara, in *Cass.,* 2002, 1015 ss.; Cass., Sez. V, 8 luglio 2008, Bassani, in *Cass.,* 2009, 3454 ss.; Cass., Sez. V, 30 settembre 2008, Romano, in *Riv. pen.*, 2009, 4, 467 ss.; Cass., Sez. V, 13 febbraio 2009, Russo, in *Cass.,* 2010, 224 ss.; Cass., Sez. V, 10 dicembre 2009, Matassich, in *Guida dir.*, 2010, 95 ss.; Cass., Sez. V, 16 febbraio 2010, Jovanovic, in *Cass.,* 2011, 6, 2198 ss.; Cass., Sez. V, 22 settembre 2010, Lesce, in *Riv. pen.*, 2011, 2, 170.

[42] Cass., Sez. V, 20 dicembre 2007, Migliazzo, in *Riv. pen.*, 2008, 6, 655 ss.; Cass., Sez. V, 29 maggio 2008, cit.; Cass., Sez. VI, 8 ottobre 2008, Peparaio, in *Cass.,* 2009, 7-8, 2828 ss.; Cass., Sez. V, 26 maggio 2009, Genchi, in *Riv. pen.*, 2010, 1, 47 ss.

dell'«oggettiva violazione delle disposizioni del titolare in ordine all'uso del sistema», mentre «irrilevanti devono considerarsi gli eventuali fatti successivi: questi, se seguiranno, saranno frutto di nuovi atti volitivi e, pertanto, se illeciti, saranno sanzionati con riguardo ad altro titolo di reato»[43]. Come osservato dalla dottrina, «il dissenso, anche tacito, del titolare dello *ius excludendi* non viene desunto, dunque, dalle finalità dell'agente, ma dall'oggettiva violazione delle disposizioni del titolare medesimo – contenute in disposizioni organizzative interne, in clausole di contratti individuali di lavoro, ovvero in norme a carattere consuetudinario o in prassi aziendali – che regolano l'accesso al sistema e che stabiliscono per quali attività e per quanto tempo la permanenza si può protrarre, mentre devono ritenersi irrilevanti, ai fini della configurazione della fattispecie, eventuali disposizioni sull'impiego successivo dei dati»[44].
Nondimeno, nel 2017, le Sezioni Unite Savarese, con specifico riferimento all'ipotesi aggravata di cui al comma 2, n. 1, hanno sposato un differente indirizzo. Tale aggravante riguarda il caso in cui il fatto sia commesso da un pubblico funzionario con abuso dei poteri o in violazione dei doveri connessi al suo ufficio o servizio. Il conflitto che la Corte era stata chiamata a comporre riguardava, in particolare, il caso in cui un pubblico ufficiale o incaricato di un pubblico servizio, utilizzando un proprio valido titolo di abilitazione, acceda o permanga in un sistema informatico o telematico per finalità estranee al proprio ufficio o servizio. I giudici di legittimità, nella loro formazione più autorevole, hanno statuito che «integra il delitto previsto dall'art. 615-*ter* c.p., comma 2, n. 1, la condotta del pubblico ufficiale o dell'incaricato di un pub-

[43] Determinanti saranno, in altri termini, solo «quelle disposizioni che regolano l'accesso al sistema e che stabiliscono per quali attività e per quanto tempo la permanenza si può protrarre, (...) mentre devono ritenersi irrilevanti, ai fini della configurazione della fattispecie, eventuali disposizioni sull'impiego successivo dei dati». Cass., Sez. un., 27 ottobre 2011, Casani, commentata da BARTOLI, *L'accesso abusivo a un sistema informatico (art. 615* ter *c.p.) a un bivio teleologicamente orientato*, in *Dir. pen. cont.*, 2012, 1, 123 ss.; FLOR, *Verso una rivalutazione dell'art. 615* ter *c.p.?*, in *Dir. pen. cont.*, 2012, 126 ss.; PECORELLA, *L'attesa pronuncia delle Sezioni unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo*, in *Cass.,* 2012, 3692 ss. Conf. Cass., Sez. V, 22 febbraio 2012, Crescenzi, in *Guida dir.*, 2012, 21, 94 ss.; Cass., Sez. II, 6 marzo 2013, Scialoia, in *Cass.,* 2014, 1, 192 ss.; Cass., Sez. V, 20 giugno 2014, Mecca, in *Riv. pen.*, 2014, 12, 1116 ss.; Cass., Sez. V, 15 gennaio 2015, P.G., in *Riv. pen.*, 2015, 7-8, 650 ss.

[44] FLOR, *La condotta del pubblico ufficiale*, cit., 509.

blico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita»[45]. Nel caso di specie, la Corte ha ritenuto immune da censure la condanna emessa nei confronti di un funzionario di cancelleria, il quale, sebbene legittimato ad accedere al registro informatizzato delle notizie di reato, conformemente alle disposizioni organizzative della Procura della Repubblica presso cui prestava servizio, aveva preso visione dei dati relativi a un procedimento penale per ragioni estranee allo svolgimento delle proprie funzioni, in tal modo realizzando un'ipotesi di *sviamento di potere*.

Tale pronuncia non è andata esente da critiche.

Si è anzitutto osservato come la Corte abbia fondato il riferito principio di diritto su «due principali equazioni: quella secondo cui quando vi è abuso vi sarebbe anche abusività dell'accesso e quella secondo cui quando vi è abuso dei poteri o violazione dei doveri le operazioni commesse sarebbero – per ricordare una categoria enucleata dalla sentenza Casani – "ontologicamente estranee" rispetto a quelle consentite»[46]. Sul punto, se è vero che la Sentenza Casani, in un passaggio intermedio, equipara alla violazione delle prescrizioni impartite dal titolare del sistema la realizzazione di «operazioni di natura ontologicamente diversa» rispetto a quelle di cui l'agente «è incaricato e in relazione alle quali l'accesso era a lui consentito», non è altrettanto vero che tale precisazione giustifica l'estensione della responsabilità ai casi di sviamento di potere. La diversità ontologica richiamata nella pronuncia del 2011, come acutamente sottolineato, «assumeva una valenza meramente negativa, riferita all'assenza di legittimazione, senza alcun riguardo per il finalismo dell'agente», «al contrario, la successiva giurisprudenza aveva utilizzato l'ontologia in un'accezione positiva come abuso di potere, in grado di esprimere il nucleo

[45] Cass., Sez. un., 18 maggio 2017, Savarese, in *Riv. it. dir. proc. pen.*, 2018, 4, 2256 ss., annotata, *inter alios*, da FASANI, *Accesso abusivo a un sistema informatico*, cit., 506 ss. e GALANTE, *L'*overruling *delle Sezioni unite in tema di accesso abusivo ad un sistema informatico*, in *Giur. it.*, marzo 2018, 735 ss.

[46] FASANI, *Accesso abusivo a un sistema informatico*, cit., 1403.

di illiceità della condotta»[47]. Nella sentenza del 2017 la configurabilità dell'art. 615-*ter*, c. 2, n. 1, c.p. viene quindi affermata in ogni caso di «"ontologica incompatibilità" dell'accesso al sistema informatico, connaturata a un utilizzo dello stesso estraneo alla *ratio* del conferimento del relativo potere»[48]. Così facendo, con «un evidente salto logico», «una circostanza aggravante fondata sulla natura agevolatoria dell'abuso rispetto alla commissione del reato viene convertita nel nucleo dell'illecito ovvero (...) viene utilizzata come chiave di lettura dell'abuso di cui al c. 1, del quale ora si predica l'irrilevanza della formale autorizzazione in presenza dello sviamento di potere». Detto altrimenti, la fattispecie aggravata di cui all'art. 615-*ter*, comma 2, n. 1, c.p., viene, di fatto, "trattata" quale reato autonomo, tradendo così la premessa fatta dalla stessa Corte circa la natura circostanziale di tale previsione[49].

Un esito interpretativo censurabile «poiché il precetto sancito dall'art. 615-*ter* rimane inalterato per tutti gli altri consociati, cui viene inibito l'accesso non autorizzato al sistema, mentre per il pubblico ufficiale e l'incaricato di un pubblico servizio assume un significato totalmente diverso»[50]. Si tratta pertanto di una soluzione difficilmente compatibile con il principio di legalità poiché i confini applicativi della fattispecie vengono dilatati esulando dal tenore letterale della norma[51]. Mettendo a dura prova il divieto di analogia *in malam par-*

---

[47] SEMINARA, *Note sul reato di accesso abusivo*, cit., 238-239.

[48] Cass., Sez. un., 18 maggio 2017, cit.

[49] Si legge nella pronuncia che «quella prevista dal comma 2, n. 1, della norma incriminatrice è qualificabile come circostanza aggravante esclusivamente soggettiva, nel senso che descrive la condotta punibile in quanto posta in essere da determinati soggetti». Cass., Sez. un., 18 maggio 2017, cit.

[50] SEMINARA, *Note sul reato di accesso abusivo*, cit., 247-249. A ciò si aggiunge – precisa l'Autore – che tale soluzione interpretativa «non appare dotata di un sufficiente fondamento politico-criminale, dovendosi dubitare della correttezza di un'equiparazione fra tutte le finalità private che abbiano ispirato l'accesso abusivo, addirittura prescindendo dal loro contenuto lecito o illecito» e «neppure va trascurato che le condotte in esame potrebbero in parte trovare un'adeguata reazione in sede disciplinare, restando esclusa la loro rilevanza penale».

[51] In tal senso, in dottrina vi è chi aveva ipotizzato «una probabile futura condanna da parte della Corte di Strasburgo per violazione dell'art. 7 della Convenzione» osservando come, fino ad allora, «se l'estensione del principio di irretroattività ai mutamenti giurisprudenziali sfavorevoli rischierebbe di generare un cortocircuito nella legalità penale, il "salvavita" del sistema che eviterebbe almeno nell'immediato la scossa – la condanna di un imputato per un fatto che solo a seguito di un *overruling* sfavorevole diventa penalmente rilevante – consiste nel riconoscimento dell'errore sul precetto». GALANTE, *L'*overruling *delle Sezioni unite in tema di accesso abusivo ad un sistema informatico*, cit., 740.

tem, viene "creata" una nuova norma incriminatrice che, anziché punire l'accesso o la permanenza non autorizzati, punisce l'utilizzo del sistema per finalità diverse da quelle dell'ufficio o del servizio[52].

Si potrebbe argomentare che in taluni casi, come in quello al vaglio delle Sezioni Unite Savarese, non sia poi così marcato il confine fra accesso o mantenimento nel sistema in violazione di disposizioni o prassi e abuso della propria facoltà di accedervi o mantenervi per perseguire finalità "personali" o che comunque esulano dalla propria attività lavorativa. Nella vicenda oggetto di detta pronuncia, il funzionario della Procura aveva fatto accesso e si era mantenuto nel registro delle notizie di reato non per svolgere la propria mansione, come disciplinata nel contratto di lavoro e precisata dalle prassi invalse, ma per consultare dati – immaginiamo – per mera curiosità o per poi comunicarli a terzi. Nondimeno, il *discrimen* fra i due approcci giurisprudenziali e i limiti dell'arresto del 2017 si apprezzano se si riflette sulle conseguenze cui essi conducono a livello probatorio. A un parametro oggettivo di valutazione dell'abusività della condotta viene sostituito un parametro soggettivo dall'applicazione incerta: un conto è provare l'oggettiva inosservanza di norme o prassi, si pensi all'accesso a parti del sistema cui l'agente non era autorizzato ad accedere o cui non era necessario accedere per svolgere la propria funzione, un altro è provare che l'agente, che ogni giorno accedeva a quel registro per ragioni d'ufficio, un giorno vi ha acceduto o vi si è mantenuto per altre finalità[53]. Come ha concluso la dottrina sul punto, «data

---

Nondimeno, la Cassazione, chiamata a pronunciarsi sul punto, ha escluso che tale interpretazione costituisca un «imprevedibile ribaltamento» dell'interpretazione della norma incriminatrice ai sensi dell'art. 7 della CEDU. Cass., Sez. V, 9 luglio 2018, Dilaghi, *Rv.* 274406.

[52] SALVADORI, *I reati contro la riservatezza informatica*, cit., 674. Cfr. FASANI, *Accesso abusivo a un sistema informatico*, cit., 1405-1406, ove si rileva che «l'equivoco sta nel fatto che le Sezioni Unite si limitano a evidenziare come lo sviamento del potere da parte del pubblico ufficiale possa essere ricondotto alle specifiche modalità di condotta tipizzate dall'aggravante, senza tuttavia osservare alcunché in merito alla prima e fondamentale sussunzione che deve essere operata: quella della condotta all'interno del primo comma dell'art. 615-*ter* c.p.».

[53] Peraltro nella giurisprudenza amministrativa sullo sviamento di potere non mancano tentativi di "oggettivazione" di tale vizio dell'atto amministrativo compiuti attraverso l'individuazione di "figure sintomatiche" del perseguimento di un fine differente da quello per il quale il potere è stato conferito al funzionario, fra cui la violazione di prassi, circolari, norme interne o l'inosservanza di limiti, parametri di riferimento e criteri per lo svolgimento dell'azione amministrativa. In argomento CASETTA, *Manuale*

l'imperscrutabilità dei fini, non è possibile muovere nessuna accusa a colui che riesca a dimostrare la parvenza di una ragione funzionale nella propria condotta, giacché le finalità private dell'azione sono destinate a emergere solo quando, successivamente, il funzionario infedele proverà a rivelare o utilizzare i segreti di ufficio acquisiti»[54], così integrando altri illeciti.

Oltre ad aver equivocato il rapporto fra ipotesi base e ipotesi aggravata, dando a quest'ultima un'interpretazione ai limiti dell'analogico, e ad aver introdotto un parametro di valutazione dell'abusività della condotta soggettivo e dall'applicazione incerta, l'orientamento delle Sezioni Unite pare viziato, nel suo *iter* argomentativo, dalla riproposizione di indirizzi ermeneutici emersi in relazione alla diversa fattispecie di abuso d'ufficio. Lo sviamento di potere è stato infatti ricondotto, per costante giurisprudenza di legittimità, alla figura criminosa di cui all'art. 323 c.p. Si è sottolineato a tale riguardo come la Cassazione nel 2017 abbia, almeno apparentemente, abbandonato «l'approccio oggettivo sostenuto dalle Sezioni Unite Casani e l'esigenza di distinguere i casi di sviamento di potere – da ricondurre in modo maggiormente coerente all'abuso d'ufficio – da quelli di strumentalizzazione del rapporto del pubblico ufficiale nell'ambito di un accesso abusivo o un mantenimento non autorizzato in un sistema informatico»[55]. Il risultato è la trasformazione dell'accesso abusivo, almeno ex art. 615-*ter*, comma 2, n. 1 c.p., in una figura criminosa "ibrida", fondata sull'eccesso o sviamento di potere, che non trova riscontro nella lettera della norma e «risulta priva di ogni fondamento anche sistematico, in quanto evoca una fattispecie che non esiste nel diritto penale,

---

di diritto amministrativo, XIII ed., Milano, 2021, 502 ss.

[54] SEMINARA, *Note sul reato di accesso abusivo*, cit., 246. Cfr. Cass., Sez. V, 20 dicembre 2007, cit.: «se (...) dovesse ritenersi che, ai fini della consumazione del reato, basti l'intenzione, da parte del soggetto autorizzato all'accesso al sistema informatico e 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».

[55] FLOR, *La condotta del pubblico ufficiale*, cit., 513, il quale censura «l'*iter* argomentativo» della pronuncia, nella misura in cui richiama, «quasi sovrapponendole, le motivazioni della decisione alla giurisprudenza di legittimità sul reato di abuso di ufficio, la quale ha ricondotto lo sviamento di potere all'interno delle nozioni di abusività della condotta».

solo che si consideri come l'art. 323 c.p. leghi il delitto di abuso d'ufficio alla produzione di un ingiusto vantaggio patrimoniale o di un danno ingiusto»[56].
La confusione fra le due fattispecie originata dalla sentenza Savarese rischia di riproporsi anche con riferimento all'attuale formulazione dell'abuso d'ufficio. Se è vero che il legislatore ha precisato che il reato viene integrato, fra l'altro, in caso di «violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità», è altrettanto vero che è stata elaborata dalla giurisprudenza di legittimità una sorta di *interpretatio abrogans* che pare ridurre di molto la portata innovativa della riforma. La Cassazione ha stabilito che la discrezionalità di cui l'agente deve godere per non rispondere deve includere la scelta dell'interesse pubblico da perseguire in concreto. Al contrario, continuerebbe a configurarsi il delitto in parola in tutti i casi in cui l'esercizio del potere discrezionale «trasmodi in una vera e propria distorsione funzionale dai fini pubblici – c.d. sviamento di potere o violazione dei limiti esterni della discrezionalità – laddove risultino perseguiti, nel concreto svolgimento delle funzioni o del servizio, interessi oggettivamente difformi e collidenti con quelli per i quali soltanto il potere discrezionale è attribuito»[57].
In conclusione, pare preferibile, come prospettato dalla dottrina, limitare l'ambito di punibilità dell'art. 615-*ter* c.p., ivi compresa l'ipotesi aggravata di cui al comma 2, n. 1, a due categorie di condotte: quelle tenute da chi «viola i limiti risultanti dal complesso delle prescrizioni previste dal titolare del sistema, in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro» e quelle di chi «compie operazioni di carattere strutturalmente differente da quelle di cui era stato incaricato e per permettere lo svolgimento delle quali gli era stato consentito l'accesso al sistema»[58].

---

[56] In questi termini SEMINARA, *Note sul reato di accesso abusivo*, cit., 248-249. Proseguendo nell'argomentazione, «l'inversione operata dalle Sezioni unite nel 2017, con cui l'abuso del c. 2, n. 1 è chiamato a sostituire quello tipizzato nel c. 1, si risolve in una trasformazione del reato di cui all'art. 615-*ter*, concepito come un abuso dell'ufficio o servizio e conseguentemente interpretato alla stessa stregua dell'art. 323 c.p.».

[57] Cass., Sez. VI, 9 dicembre 2020, Garau, in *Penale diritto e procedura*, 19 gennaio 2021, con nota di ROMANO, *Il "nuovo" abuso d'ufficio e l'*abolitio criminis *parziale*.

[58] PLANTAMURA, *Domicilio e diritto penale*, cit., 206.

5. La riformulazione della norma da parte del VII Gruppo di lavoro sulla riforma dei reati contro la persona. Partendo dalle riflessioni critiche presentate in occasione del Convegno di Torino del 9 e 10 novembre 2018 e riprese nel successivo Convegno di Napoli del 30 e 31 maggio 2019 con riferimento alle "fattispecie penali in materia di violazioni della riservatezza e sicurezza informatiche", fra cui l'art. 615-*ter* c.p., sono state avanzate proposte di riformulazione volte a superarne i limiti applicativi e sistematici, a renderle più aderenti all'evoluta realtà fenomenologica e alle indicazioni contenute nelle fonti sovranazionali nonché di più immediata comprensione per operatori giuridici e cittadini[59].

La proposta elaborata in vista del seminario AIPDP del 10 settembre 2021 dal Gruppo di lavoro sui "reati contro l'inviolabilità del domicilio, la tutela della vita privata e dei segreti, la libertà e la personalità informatica" prevede anzitutto la creazione di una nuova e autonoma «Sezione VI», da aggiungere all'interno del capo III («Dei delitti contro la libertà individuale») del Titolo XII («Dei delitti contro la persona») del Libro II del codice penale, denominata «Dei delitti contro la riservatezza e la sicurezza informatiche». Come anticipato, la necessità di conferire un'autonomia anche sistematica, oltre che strutturale, ai reati informatici in "senso stretto" è da tempo avvertita dalla dottrina[60], pur senza ignorare, in virtù della concezione personalistica che informa la tutela penale dei beni giuridici, la stretta connessione con la tutela della libertà morale della persona cui i "nuovi beni" da proteggere sono riferibili[61].

---

[59] PICOTTI, FLOR, SALVADORI, Proposta di riforma dei *Reati contro l'inviolabilità del domicilio, la tutela della vita privata e dei segreti, la libertà e la personalità informatica*, 1-2, liberamente fruibile su *www.aipdp.it*. In particolare, fra le fonti sovranazionali richiamate nella proposta: la "Convenzione del Consiglio d'Europa sulla criminalità informatica" (2001), che fa espressamente riferimento ai principi di "confidenzialità, integrità e disponibilità" dei dati e dei sistemi informatici; la Direttiva 2013/40/UE, relativa agli attacchi ai sistemi di informazione; e la Direttiva 2016/1148/UE, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione.

[60] L'assetto attuale dei reati informatici viene descritto dai proponenti come «miscela di anacronismi, meccanismi evolutivi e mutazioni genetiche indotti dai fattori esogeni ed endogeni più diversi». FIORE, Proposta di riforma de *I reati contro il diritto alla riservatezza*, 1, liberamente fruibile su *www.aipdp.it*.

[61] PICOTTI, FLOR, SALVADORI, Proposta di riforma, cit., 2-3. Si legge nella proposta: «gli aspetti specifici che caratterizzano tali beni, qualificati dall'intreccio strettissimo con le concomitanti esigenze di tutela delle reti e dei sistemi informatici, che necessariamente veicolano le odierne forme di espressione, ge-

Con specifico riferimento alla fattispecie di accesso abusivo a sistema informatico o telematico, in linea con l'orientamento dottrinale maggioritario, si propone di superare la sua configurazione come reato di danno posto a tutela del domicilio informatico, lasciando la nozione di domicilio alla sua tradizionale declinazione «fisico-spaziale» e «abbandonando la forzosa estensione anche a quella "*informatica*", che era stata operata in una fase di primo approccio alla nuova realtà tecnologica dal legislatore del 1993». L'ipotesi delittuosa andrebbe invece concepita come fattispecie posta a tutela della riservatezza informatica[62] «intesa quale "*confidenzialità*" (non segretezza in senso stretto) e "*disponibilità*" dei dati, dei sistemi e delle stesse reti (in sintesi: di "spazi" informatici, ovunque si trovino, anche nel c.d. *cloud*), di pertinenza non solo di una persona fisica, ma anche di un ente o di una persona giuridica»[63].

---

stione, trattamento della comunicazione e diffusione dei dati e informazioni nel *Cyberspace*, superando e assorbendo i profili di interrelazione immediatamente o esclusivamente "fra persone" (basti pensare al ruolo che oggi svolgono i sempre più sofisticati algoritmi, sistemi di intelligenza artificiale e *machine learning* nella stessa elaborazione, selezione, indirizzamento di informazioni e trasmissioni il cui input soltanto può essere originariamente "personale"), porta a ritenere prevalente l'esigenza di autonomia anche sistematica, oltre che strutturale, delle nuove fattispecie, così in grado, fra l'altro, di esercitare un più chiaro ruolo di richiamo e attenzione sia verso i destinatari, sia verso gli operatori giuridici (pubblici ministeri, giudici, forze di polizia, avvocati), per le predette nuove e peculiari esigenze di protezione penale. Si tratta di delitti che offendono beni comunque riferibili alla persona, intesa in un senso molto ampio e indiretto, essendovi sempre, "dietro" le comunicazioni e i trattamenti informatici, una persona umana o un ente: per cui si giustifica (almeno allo stato) la collocazione nel Titolo XII, e in specie nel Capo III dedicato alla "Libertà morale"».

[62] Sebbene non senza riserve, il bene giuridico della riservatezza informatica è stato ritenuto dai proponenti «quello che più di altri e meglio di altri ha saputo nel tempo assumere una "identità" tale da renderlo immediatamente riconoscibile e anche per questo presenta una indubbia attitudine a polarizzare un universo valoriale che nel tempo è divenuto patrimonio comune degli ordinamenti nazionali e anche di quelli sovranazionali». In quanto oggetto «di approfondita elaborazione da parte sia delle Corti nazionali (anche costituzionali), che di quelle sovranazionali, in virtù della sua stabile presenza nelle carte dei diritti e questa solida identità rende in prospettiva meno difficile scrivere norme», non pare correre il «rischio degli eccessi definitori o peggio del cedimento a derive casistiche, perché nella fase di adattamento interpretativo delle norme alla fenomenologia reale si può contare sulla "guida" di un concetto forte e allo stesso tempo già raffinato, grazie alla sua elaborazione anche applicativa. La riservatezza, in altri termini, in un settore dove le dinamiche di bilanciamento riguardano con frequenza interessi disomogenei, sembra garantire, insieme a punti di riferimento certi e stabili sul piano normativo, anche spazi di valutazione dotati di adeguata capacità di conformarsi alla realtà». FIORE, Proposta di riforma, cit., 2-3.

[63] PICOTTI, FLOR, SALVADORI, Proposta di riforma, cit., 4. In particolare, la nuova Sezione dovrebbe

Passando alla nuova formulazione dell'art. 615-*ter* c.p., si propone di punire, sempre «a querela della persona offesa» e «con la reclusione fino a tre anni», «chiunque accede senza autorizzazione o eccedendone i limiti ad un sistema informatico o ad una sua parte». La riforma riguarderebbe anche la rubrica, modificata da "accesso abusivo ad un sistema informatico o telematico" ad "accesso non autorizzato ad un sistema informatico". Verrebbe quindi soppresso l'aggettivo "telematico", in quanto «il concetto di "sistema informatico" è di per sé idoneo a ricomprendere anche i sistemi di elaborazione tra loro interconnessi o connessi alla rete Internet», e si rimedierebbe all'inadeguatezza lessicale, più volte stigmatizzata dai commentatori, del verbo "introdursi". Ancora, verrebbe superato il binomio "introduzione e mantenimento", in quanto «causa di notevoli problemi ed equivoci in giurisprudenza e in dottrina», limitando l'incriminazione alla condotta di "accesso non autorizzato" sull'assunto della sua idoneità a ricomprendere anche i casi di permanenza non autorizzata nel sistema.

Al contempo, si è ritenuto di espungere il riferimento alle misure di sicurezza in quanto «la previsione, quale requisito tipico di fattispecie, della *oggettiva violazione delle misure di sicurezza* poste a protezione del sistema, porterebbe a escludere la rilevanza penale delle condotte sempre più frequenti dei dipendenti, dei funzionari pubblici e, più in generale, dei c.d. *insider* che, eccedendo i limiti dell'accesso consentito, accedono a spazi o ambiti non protetti di un sistema informatico (di un *Cloud*, di un *Server*, di una banca dati, ecc.) per consultare, copiare, comunicare o danneggiare dati ed informazioni», «dal momento che l'iniziale *accesso* al sistema avviene attraverso l'impiego legittimo delle credenziali di autenticazione, compresa la *password*, fornite dal datore di lavoro o dal titolare del sistema»[64].

---

ospitare tre gruppi di delitti: quelli contro la riservatezza informatica (fra cui gli attuali artt. 615-*ter* c.p., 615-*quater* c.p., 616, ultimo comma, c.p., 623-*bis* c.p., 617-*quater* c.p., 617-*quinquies* c.p., tutti da emendare), quelli contro la sicurezza informatica (fra cui gli attuali artt. 615-*quinquies* c.p., 635-*bis* c.p., 635-*ter* c.p., 635-*quater* c.p., 635-*quinquies* c.p.) e, in un gruppo a sé, la nuova fattispecie di "violazione dell'identità digitale", «con contestuale abrogazione dell'attuale comma 3 dell'art. 640-*ter* c.p., che è oggi applicabile alla sola frode informatica, quale sua ipotesi aggravata, ma che invece, debitamente riformulato, dovrebbe avere una portata generale, assorbendo anche lo spazio oggi affidato dalla giurisprudenza al più lieve reato di sostituzione di persona, di cui all'art. 494 c.p.».

[64] *Ivi*, 7. Inoltre, «l'espressa incriminazione del semplice "accesso" non autorizzato (o "abusivo"), in

Ancora, il carattere *abusivo*, o meglio "*non autorizzato*", dell'accesso – viene specificato – dovrebbe essere inteso in senso oggettivo, sulla base della «violazione di specifici regolamenti interni, norme o disposizioni aziendali anche di natura contrattuale o comunque norme extrapenali, pur non necessariamente specifiche per la regolazione degli accessi, ma inerenti alle finalità e ai contenuti delle mansioni affidate, sulla cui base si possa anche determinare in modo chiaro a quali spazi della memoria o del sistema o a quali dati e archivi il dipendente o l'incaricato possa accedere nell'esercizio delle sue mansioni o per le "ragioni" o funzioni per cui l'accesso è consentito». La "*mancanza di autorizzazione*" andrà quindi interpretata come «*clausola di illiceità speciale*, che contribuisce alla tipizzazione oggettiva del fatto di reato», scongiurando quegli orientamenti ermeneutici che hanno attribuito rilevanza alle «finalità personali o soggettive dell'*insider*»[65].

Con riferimento alle ipotesi aggravate, per cui si procede d'ufficio, la pena della reclusione, sempre da uno a cinque anni, sarebbe ancora prevista per il pubblico ufficiale o incaricato di un pubblico servizio che abbia commesso il fatto con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di amministratore (figura di nuova introduzione) od operatore di sistema. In secondo luogo, un trattamento sanzionatorio aggravato è previsto, nella nuova formulazione, per chi abbia commesso il fatto con violenza sulle cose (non più sulle persone o essendo palesemente armato) o (ipotesi nuova) ponendo in essere interferenze non autorizzate in ambito informatico[66]. Verrebbe invece abrogata l'aggravante prevista attual-

luogo dell'attuale "introdursi", oltre ad essere più coerente con il riferimento all'ipotesi che avvenga anche soltanto "a una parte" di un sistema informatico, presenterebbe il vantaggio di permettere l'incriminazione degli accessi abusivi realizzati non solo dai c.d. *outsider* (ad es. *hacker* e *cracker*), ma anche dai dipendenti, incaricati o, in generale, *insider* che, possedendo legittimamente le credenziali di autenticazione per "introdursi" in un sistema informatico, si spingono però oltre i limiti dell'autorizzazione e operano ulteriormente, accedendo "senza autorizzazione" anche a parti o "spazi" riservati, che sarebbero loro preclusi dal titolare o dall'ambito delle loro competenze».

[65] *Ivi*, 8.

[66] *Ivi*, 9. A questo proposito viene specificato che «la modalità della "violenza sulle cose" deve estendersi anche alle specifiche "interferenze non autorizzate in ambito informatico" quali definite oggi dal comma 3 dell'art. 392 c.p. e impropriamente ricondotte alla nozione di "violenza" c.d. informatica». Mentre i

mente al comma 3 e relativa al caso in cui dal fatto derivi «la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti»[67]. Aggravamenti di pena più severi sarebbero poi previsti per i fatti che riguardino sistemi informatici di pubblica utilità o di una infrastruttura critica (parzialmente in linea con quanto attualmente previsto) nonché (ipotesi di nuova introduzione) qualora il fatto sia commesso nell'ambito di un'associazione per delinquere.

6. *Alcune considerazioni sulla proposta di «accesso non autorizzato ad un sistema informatico»*. In relazione alle predette prospettive di riforma della fattispecie disciplinata dall'art. 615-*ter* c.p., anche alla luce dell'elaborazione dottrinale e giurisprudenziale in materia, possono essere sviluppate alcune riflessioni.

È bene premettere che regolare compiutamente i reati informatici possa sembrare un'utopia. La velocità con cui si evolvono le nuove tecnologie digitali, e quindi con cui muta la fenomenologia delle offese perpetrate attraverso i dispositivi informatici e la rete, rischia di rendere obsoleta ogni norma già durante il suo *iter* di approvazione. È tuttavia indubbio che il divario tecnologico che separa gli anni Novanta dai giorni nostri rende imprescindibile un aggiornamento della normativa[68].

---

casi di "violenza alla persona" e commissione del fatto da parte di soggetto "palesemente armato", anche alla luce dell'evoluzione tecnologica e digitale, risultano pressoché privi di riscontri nella prassi giurisprudenziale.

[67] Tale scelta è animata dal fine di superare tale «controversa ipotesi di reato aggravato dall'evento», ferma restando, nel caso in cui l'accesso non autorizzato sfoci in danneggiamento del sistema informatico, l'applicabilità della disciplina sul concorso di reati. *Ibidem*, 9.

[68] Viene sottolineato dalla dottrina l'«affanno con il quale il legislatore è costretto ad adeguarsi ai mutamenti della sottostante cornice empirico-criminologica, sempre più contraddistinta da forme di aggressione tecnologicamente raffinate, insidiose e non di rado oscure», da cui scaturisce «l'immagine di un sistema in continua fibrillazione, alla sfiancante rincorsa di correttivi, aggiustamenti e integrazioni, che, spesso, fomentano dissimmetrie sistematiche e ragguardevoli aporie interpretative». PIERGALLINI, *I delitti contro la riservatezza informatica*, cit., 712. Così: «il diritto penale dell'informatica costituisce un insieme ancora eterogeneo e sovrabbondante di norme incriminatrici, frutto di ripetuti interventi settoriali e frammentari, privi di una meditata elaborazione dogmatica e non sempre coerenti con la realtà empirico-criminologica che caratterizza questo peculiare settore di criminalità». SALVADORI, *I reati*

Con specifico riferimento alla riformulazione dell'accesso abusivo a sistema informatico o telematico, vanno salutate con favore sia l'eliminazione del verbo «introdursi», scelta lessicale impropria del legislatore del 1993, sia l'espunzione dell'aggettivo «abusivo» e, correlativamente, dell'avverbio «abusivamente», fonte di non poche *querelle* ermeneutiche, preferendo la dizione «accesso non autorizzato» nella rubrica così come nel testo della norma[69].

Per quanto concerne il superamento del binomio "accesso" - "permanenza" nel sistema informatico, il rischio è quello che resti impunita la condotta di chi, autorizzato ad accedere al sistema per eseguire una o più specifiche operazioni, vi si protragga *inviso domino* oltre il tempo necessario, mettendosi così nelle condizioni di prendere visione di contenuti o di svolgere ulteriori attività. Non pare scontato che tale ipotesi rientri nella locuzione di nuovo conio di «accesso non autorizzato», per quanto lata, se non attraverso estensioni interpretative di dubbia compatibilità con il principio di legalità.

Parimenti, la specificazione «protetto da misure di sicurezza», riferita al sistema informatico in cui deve avvenire l'accesso affinché il reato possa ritenersi integrato, che si propone di elidere, pare conservare una sua utilità in quei casi in cui è particolarmente complesso desumere l'autorizzazione all'accesso o il difetto della stessa, non sussistendo regolamenti o prassi invalse. Si pensi a quei dispositivi che, siti in luoghi "promiscui" in cui transitano, ad esempio, personale scolastico e studenti, piuttosto che dipendenti dell'azienda e terzi, potrebbero essere utilizzati, anche in buona fede, da soggetti non autorizzati, se non fosse richiesta l'autenticazione con credenziali e password. Oppure si pensi a molti "luoghi della rete", siano essi banche dati, forum o *social network*, in cui solo la predisposizione di "barriere" può far intuire all'utente che l'accesso è autorizzato solo agli abbonati, agli iscritti e via dicendo[70]. In dottri-

---

contro la riservatezza informatica, cit., 656. Con specifico riferimento al delitto di cui all'art. 615-*ter* c.p. si è affermato che «i tratti criminologici del reato, seguendo necessariamente l'evoluzione tecnologica a cui si ancorano, sembrano assoggettati a una costante variazione». BUSSOLATI, *Accesso abusivo a un sistema informatico o telematico*, cit., 428.

[69] Anche la "Convenzione del Consiglio d'Europa sulla criminalità informatica" del 2001, all'art. 2, rubricato «accesso illegale a un sistema informatico», si riferisce, nel testo, a chi accede a un sistema «senza autorizzazione».

[70] Si veda sul punto PLANTAMURA, *Domicilio e diritto penale*, cit., 191 ss.

na si è osservato a tal proposito come il richiamo alle misure di sicurezza sia un elemento fondamentale che garantisce la determinatezza della fattispecie, consente l'accertamento dell'elemento soggettivo e segna un punto di equilibrio fra le istanze di tutela sottese all'incriminazione dell'accesso abusivo e la libertà di accesso a dati, programmi e spazi virtuali[71].

Altre considerazioni riguardano la formulazione lessicale, pressoché inalterata nella proposta di riforma, dell'aggravante di cui al comma 2, n. 1), riferita ai fatti commessi da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio. Attorno a tale previsione, come illustrato, è andata consolidandosi un'opzione interpretativa, sposata dalle Sezioni Unite Savarese, oggetto di non poche (condivisibili) critiche. In particolare, si è assistito alla sovrapposizione del carattere abusivo dell'accesso o permanenza nel sistema informatico con il cd. sviamento di potere, ossia il perseguimento da parte del pubblico funzionario di finalità estranee all'ufficio o al servizio, disattendendo così l'insegnamento delle Sezioni Unite Casani che, per l'ipotesi base, avevano cristallizzato il criterio oggettivo della contrarietà a prescrizioni o normative interne o l'ontologica estraneità delle operazioni compiute rispetto all'obiettivo per cui l'agente era stato autorizzato all'accesso. A tal proposito, in dottrina è stato rilevato come «l'art. 615-*ter*, c. 2, n. 1 appare formulato in termini assai problematici, non essendo chiaro il rapporto che intercorre tra l'abuso ex c. 1, caratterizzante l'introduzione o il mantenimento nel sistema, e l'abuso dei poteri tipizzato nel c. 2, n. 1 insieme alla violazione dei doveri funzionali»[72]. Al contempo, proprio a partire dalle perplessità suscitate dalla predetta pronuncia di legittimità, taluno ha auspicato «una (pur improbabile) riforma dell'art. 615-*ter* c.p., tesa a chiarire definitivamente gli elementi della fattispecie che hanno dato adito alla [relativa] questione di diritto (...), preferibilmente in via restrittiva (...). E ciò al fine di evitare che (...) il cittadino si trovi nell'impossibilità di comprendere se verrà considerata penalmente rilevante

[71] PICOTTI, voce *Reati informatici*, cit., 22. Cfr., SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigma dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in *Tutela penale della persona e nuove tecnologie*, cit., 144; ID., *I reati contro la riservatezza informatica*, cit., 677.

[72] SEMINARA, *Note sul reato di accesso abusivo*, cit., 236.

la condotta di chi, essendo abilitato ad accedere a un sistema informatico e senza violare alcuna disposizione di natura oggettiva, visualizzi contenuti a lui accessibili, per finalità difformi da quelle che legittimano tale autorizzazione»[73].

Al fine di meglio chiarire i confini applicativi della fattispecie aggravata, in linea con i principi di precisione e tassatività, si potrebbe pensare alla sua riformulazione, precisando che «l'abuso dei poteri o la violazione dei doveri devono rappresentare la modalità attraverso la quale il soggetto qualificato ha ottenuto l'accesso al sistema informatico o si è mantenuto in quest'ultimo»[74] e non le finalità perseguite. Tale specificazione, unita all'elisione dell'avverbio "abusivamente", contribuirebbe a scongiurare derive interpretative come quella accolta dalle Sezioni Unite Savarese. Un'alternativa, anche se meno convincente ed efficace nel neutralizzare tali rischi, potrebbe consistere nel superamento dell'aggravante speciale, per evitare che venga surrettiziamente trasformata in (o trattata come) reato autonomo, potendo comunque trovare applicazione l'aggravante comune di cui all'art. 61, n. 9, c.p. Il pubblico ufficiale o incaricato di pubblico servizio che acceda o permanga in un sistema informatico per finalità estranee all'ufficio o al servizio, d'altronde, potrebbe sempre rispondere sul piano disciplinare oppure, se ne ricorrono gli elementi costitutivi, potrebbe integrare altri reati come l'abuso d'ufficio, la rivelazione di segreti d'ufficio, la corruzione per l'esercizio della funzione, nonché illeciti (anche penali) in materia di protezione dei dati personali[75].

In relazione alla figura, di nuova introduzione, dell'«amministratore di sistema», sarebbe forse opportuno ancorarla, a beneficio del principio di precisione, a una definizione normativa, anche al fine di distinguerla da quella di «operatore di sistema», già menzionata nell'attuale formulazione della norma[76]. Anche all'«abuso» di tali qualità (quella di amministratore e quella di

[73] FASANI, *Accesso abusivo a un sistema informatico*, cit., 1407.

[74] In questi termini SALVADORI, *I reati contro la riservatezza informatica*, cit., 685.

[75] Cfr. SEMINARA, *Note sul reato di accesso abusivo*, cit., 247-249; FLOR, *La condotta del pubblico ufficiale*, cit., 512-515.

[76] Nella proposta di riforma si precisa che la locuzione «"amministratore di sistema" («*system administator*») indica quei soggetti qualificati anche sul piano tecnico-informatico che, avendo il controllo delle fasi del processo di elaborazione e trattamento di dati informatici, possono disporre l'accesso con mag-

operatore di sistema), quale fonte di aggravamento del trattamento sanzionatorio, dovrebbe peraltro estendersi la specificazione che lo stesso deve intendersi come riferito alle modalità dell'accesso o del mantenimento non autorizzato e non alle finalità perseguite dall'agente, prevenendo così interpretazioni "soggettive" "alla Savarese".

7. *Spunti per un ripensamento dell'interesse protetto alla luce della teoria del bene giuridico.* Vale la pena, a questo punto, di dedicare alcune riflessioni al bene giuridico che, nella proposta di riforma, sarebbe presidiato dalla fattispecie di cui all'art. 615-*ter* c.p., ossia la *riservatezza informatica*.
Il nuovo bene giuridico non coinciderebbe né con il domicilio informatico, né con la riservatezza *tout court*, né con la segretezza, ma andrebbe inteso come «*potestà di escludere terzi* e di essere garantiti contro intrusioni indesiderate e interferenze potenzialmente dannose o comunque non consentite, per salvaguardare un proprio "*spazio informatico*" libero, autonomo e sicuro, in cui possa svolgersi senza impedimenti la propria personalità, che opera tramite relazioni e attività dislocate nella rete»[77]. Si tratterebbe di un bene giuridico più ampio della riservatezza *tout court*, che non si esaurirebbe nella protezione della persona da accessi abusivi nel suo "domicilio informatico", inteso come spazio ideale, ma anche fisico, in cui sono contenuti i dati informatici di pertinenza dell'individuo[78], ma mirerebbe a garantire «la *sicurezza* e l'*esclusività* dell'accesso, della gestione e della disponibilità del suo spazio informatico, o meglio cibernetico, vale a dire delle risorse informatiche con l'eventuale insieme di dati di sua pertinenza esclusiva contro ogni interferenza e danneggiamento, essendo l'interesse meritevole di tutela comprensivo della *confidenzialità, sicurezza* e dunque *libertà* delle azioni ed elaborazioni, anche solo potenziali o future, realizzabili nel "proprio" ambito *esclusivo*»[79].

---

giore facilità ai sistemi informatici sui quali hanno competenza». PICOTTI, FLOR, SALVADORI, Proposta di riforma, cit., 9.

[77] PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, cit., 59-60.

[78] Cass., Sez. V, 8 maggio 2012, P.L., in *Dir. inform.*, 2013, 86 ss.

[79] PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, cit., 60-61. L'Autore adotta la locuzione "spazio cibernetico", preferendola alle espressioni "spazio virtuale" e "spazio informatico", in quanto maggiormente efficace a indicare uno spazio reale, ma non necessariamente coinci-

La riservatezza informatica meglio si attaglierebbe alla nuova fenomenologia del *cybercrime* dei "beni tradizionali" in quanto avrebbe «ad oggetto l'interesse all'esclusività dell'accesso a uno o più spazi informatici, a prescindere dalla natura dei dati e delle informazioni ivi archiviati, nonché alla loro disponibilità rispetto a illegittime interferenze da parte di terzi soggetti». In particolare, viene richiamata dalla dottrina una «"teoria assiomatica" delle aree di tutela della riservatezza, che va oltre l'originaria contrapposizione fra la sfera individuale e quella privata, intese quali componenti del generale diritto della personalità, per la presenza di aree di pertinenza dell'individuo, ovvero di "spazi informatici" di manifestazione della sua personalità, che coincidono con l'interesse sostanziale alla protezione di informazioni, siano esse riservate o non riservate, e al loro controllo nello svolgimento di rapporti giuridici e personali *off-line*, *on-line* o in altri "*cyberspaces*"». Così concepita, la riservatezza informatica tutelerebbe sia «l'interesse del singolo» sia «quello super-individuale o di natura collettiva a che l'accesso a sistemi informatici e alla stessa rete avvenga per finalità lecite e in modo tale da essere regolare per la sicurezza degli utenti»[80].

Richiamando il principio di "confidenzialità", che, accanto a quello di integrità e di disponibilità dei dati e dei programmi informatici costituisce uno dei pilastri attorno ai quali ruota la "Convenzione sulla criminalità informatica" del 2001, la riservatezza informatica rappresenta indubbiamente parte integrante dell'orizzonte valoriale cui informare la tutela penale degli interessi afferenti ai sistemi e alle comunicazioni informatiche e telematiche[81], viene però

---

dente con un sistema informatico o con un computer, potendosi anche trattare di un *social network* o di altri servizi direttamente accessibili attraverso server connessi in rete.

[80] FLOR, *La condotta del pubblico ufficiale*, cit., 512. Cfr. SALVADORI, *I reati contro la riservatezza informatica*, cit., 664, ove si sottolinea che «non si tratta pertanto di tutelare, mediante la previsione dei reati contro la riservatezza informatica, il solo *ius excludendi alios* del titolare del sistema, ma indirettamente anche l'interesse collettivo al regolare funzionamento, alla integrità e alla disponibilità dei sistemi (c.d. sicurezza informatica)». Così la riservatezza informatica assurgerebbe, in definitiva, a nuovo diritto fondamentale dell'uomo, quale manifestazione del diritto generale allo sviluppo della personalità, che si fonda sull'art. 2 Cost. e, più specificamente, sull'art. 8 della CEDU e sugli artt. 8 e 9 della Carta dei diritti fondamentali dell'Unione europea, e di cui sono espressione anche il diritto inviolabile al domicilio, al rispetto della vita privata e familiare, alla segretezza delle comunicazioni e la stessa libertà di manifestazione del pensiero.

[81] Si è messo in evidenza come «la riservatezza digitale o informatica» venga «configurata dal nuovo con-

da chiedersi se tale locuzione sia del tutto adeguata, a prescindere dai significati che le vengono attribuiti, a indicare l'interesse tutelato dall'art. 615-*ter* c.p.[82].

Non è questa la sede per ripercorrere il dibattito sulla teoria del bene giuridico, dibattito «tra i più complessi e articolati di tutta la scienza penalistica»[83], basti richiamare, ai presenti fini, le principali funzioni attribuite a tale categoria. Nella manualistica si suole distinguere fra funzione *politico-garantista*[84],

---

testo normativo dando vita a un vero e proprio "*Statuto penale della riservatezza digitale*", assolutamente indispensabile per utilizzare in maniera conforme il principio di proporzione della norma penale e della conseguente sanzione». TRONCONE, *La tutela penale della riservatezza e dei dati personali. Profili dommatici e nuovi approdi normativi*, Napoli, 2020, 59-60.

[82] Anche chi, in dottrina, è favorevole all'individuazione del diritto alla riservatezza quale oggetto di tutela dei reati informatici, individuandone «l'ossatura» «nella libertà dell'individuo di determinare le modalità di costruzione della propria sfera privata», riconosce che si tratti di un diritto, *prima facie*, «non agevolmente perimetrabile» e che «trova nel sistema penale una tutela la cui ampiezza risente del carattere inevitabilmente (e doverosamente) "frammentario" del diritto penale». PIERGALLINI, *I delitti contro la riservatezza informatica*, cit., 714.

[83] In questi termini FORTI, *L'ordinamento lessicale dei beni giuridici personali nella parte speciale del codice penale*, in *Tutela penale della persona e nuove tecnologie*, cit., 370.

[84] In relazione alla funzione critico-selettiva del bene giuridico, che attribuisce a tale categoria il ruolo di paradigma assiologico di contenimento della sfera di previsione penale, è d'obbligo il rimando a Roxin, che considera beni giuridici tutti quei dati o obiettivi di scopo (*Zwecksetzungen*) necessari per il libero sviluppo della persona, per la realizzazione dei suoi diritti fondamentali e per il funzionamento di un sistema statuale fondato su tale rappresentazione di scopo. ROXIN, GRECO, *Strafrecht. Allgemeiner Teil*, München, 2020, 9 ss. (Sulle condizioni di legittimazione della tutela penale e sulla rilevanza assunta a tal fine dalla teoria del bene giuridico si vedano, *ex multis*, PALAZZO, *I confini della tutela penale: selezione dei beni e criteri di criminalizzazione*, in *Riv. it. dir. proc. pen.*, 1992, 453 ss. e FORTI, *Principio del danno e legittimazione "personalistica" della tutela penale*, in *Sulla legittimazione del diritto penale. Culture europeo-continentale e anglo-americana a confronto*, a cura di Fiandaca, Francolini, Torino, 2008, 43 ss.). Nondimeno, la definizione di bene giuridico più ricorrente nella manualistica è la cd. "definizione situazionale" elaborata da Jäger (JÄGER, *Strafgesetzgebung bei Rechtsgüterschutz und Sittlichkeitsdelikten*, Stuttgart, 1957, 13), in virtù della quale i beni giuridici sono «situazioni di fatto permeate di valore, che possono essere modificate e che perciò possono essere tutelate contro tali modificazioni; in una parola sono situazioni di fatto, offendibili, tutelabili». MARINUCCI, DOLCINI, GATTA, *Manuale di diritto penale. Parte generale*, cit., 10. Ancora, merita di essere menzionata la definizione di bene giuridico quale «*entità percepita come valore in un determinato contesto sociale e culturale*, suscettibile di *lesione o messa in pericolo* ad opera di condotte dell'uomo e per questo ritenuta dal legislatore meritevole di tutela anche in sede penale». DE VERO, *Corso di diritto penale*, Torino, 2020, 123. Quanto alla "meritevolezza" di tutela, va richiamata la teoria costituzionalmente orientata del bene giuridico, che fa dipendere l'innalzamento di un interesse al rango di bene giuridico dalla sua rilevanza costituzionale diretta o indiretta. Cfr. BRICOLA, *Teoria generale del reato*, in *Novissimo digesto italiano*,

vale a dire di «critica nei riguardi delle scelte di politica criminale» e di limite alla potestà punitiva dello Stato; funzione *sistematica* (o *classificatoria*), che sottolinea la tendenza degli stati moderni ad assumere «a criterio identificativo di una serie di incriminazioni, ritenute omogenee, proprio il bene offeso dai rispettivi illeciti»; funzione *interpretativa*, esplicata nei confronti dell'interprete, «nel senso che la norma incriminatrice non può trovare applicazione se non è ravvisabile nel caso concreto l'offesa dell'interesse che il legislatore ha inteso tutelare in via generale e astratta», colmando eventuali scarti fra «significato letterale e vocazione di tutela della fattispecie»; funzione *dogmatica*, intesa come «utilità della categoria ai fini della corretta applicazione di talune norme, che in mancanza di tale aggancio resterebbero esposte a rischi di equivocità e incertezza»[85].

Sebbene la rilevanza del bene giuridico sia stata oggetto di critiche e ridimensionamenti[86], non si può non riconoscerne il valore politico-criminale ed ese-

XIX, Torino, 1973, 15 ss.; ANGIONI, *Contenuto e funzioni del concetto di bene giuridico*, Milano, 1983, 152 ss. Per quanto tale teoria non sia andata immune da critiche, le va riconosciuto il merito di aver contribuito alla sensibilizzazione degli studiosi rispetto ai profili costituzionali dell'illecito penale. Sul punto, *inter alios*, M. DONINI, *Il volto attuale dell'illecito penale*, Milano, 2004, 66 ss. e MANES, *Il principio di offensività nel diritto penale*, Torino, 2005, 41 ss.

[85] DE VERO, *Corso di diritto penale*, cit., 123 ss. Con riferimento alla funzione dogmatica, la corretta individuazione dell'interesse tutelato è essenziale, ad esempio, per l'identificazione della persona offesa, che rileva in relazione «a vari momenti di disciplina sia di carattere sostanziale che processuale». *Ivi*, 128. Fra i profili dommatici legati alla teoria del bene giuridico vengono poi richiamati la teoria della pena, il tentativo inidoneo e il reato impossibile, il concorso di norme, ecc. MERLI, *Introduzione alla teoria generale del bene giuridico. Il problema. Le fonti. Le tecniche di tutela penale*, Napoli, 2006, 20-21.

[86] Un approccio critico si ravvisa, ad esempio, in Fiandaca (FIANDACA, *Il "bene giuridico" come problema teorico e come criterio di politica criminale*, in *Riv. it. dir. proc. pen.*, 1982, 43 ss.; ID., *Sul bene giuridico. Un consuntivo critico*, Torino, 2014) e in Romano, il quale, pur ridimensionando la valenza "delimitativa" del potere punitivo del bene giuridico, sottolinea come «ai beni giuridici devono riconoscersi non trascurabili funzioni: una funzione dogmatica, utile per la ricognizione del sistema penale; una funzione classificatoria, al fine del raggruppamento dei reati in un ordine legale che rispecchi una tendenziale gerarchia di valori; una funzione interpretativa, di aiuto, dall'esterno del reato, alla comprensione del suo significato». ROMANO, *La legittimazione delle norme penali: ancora su limiti e validità della teoria del bene giuridico*, in *Criminalia*, 2011, 43. Sulla «crisi del bene giuridico» si vedano altresì DONINI, *Teoria del reato. Una Introduzione*, Padova, 1996, 131 ss.; PALAZZO, *I confini della tutela penale*, cit., 459 ss.; FORTI, *Per una discussione sui limiti morali del diritto penale, tra visioni liberali e paternalismi giuridici*, in *Studi in onore di Giorgio Marinucci*, a cura di Dolcini, Paliero, Milano, 2006, 290 ss.; MERLI, *Introduzione alla teoria generale del bene giuridico*, cit., 92 ss.

getico-applicativo (quale punto di riferimento per l'interpretazione teleologica delle norme vigenti). Come anticipato[87], l'emersione di nuovi interessi determinata dall'evoluzione sociale, culturale e tecnologica gioca un ruolo tutt'altro che secondario nelle scelte di criminalizzazione in astratto così come nelle traiettorie interpretative e applicative delle fattispecie di nuovo conio. A tal proposito si è osservato come «riconoscere che i beni giuridici sono storicamente condizionati equivale ad ammettere che essi nascono e muoiono a seconda delle rappresentazioni culturali e/o delle intese sui valori che emergono nella società nei diversi periodi», così «i beni non sono creati di volta in volta dal legislatore a suo piacimento», «non sono un suo "prodotto"», bensì «preesistono al legislatore, al quale spetta di interpretare i segnali che, provenendo dalla società, gli additano concreti valori da proteggere mediante leggi anche penali»[88]. Il bene giuridico riveste quindi un ruolo significativo nella configurazione delle fattispecie incriminatrici e quale «filo conduttore per l'interpretazione»[89] delle stesse, collegando il diritto penale alla realtà empirico-sociale[90]. Del resto, è innegabile che «qualunque riforma di parte speciale del codice penale che ambisca a incidere sulla realtà dei bisogni di tutela espressi dal corpo sociale» debba «preliminarmente sapere "cosa" proteggere da "cosa"»[91].

---

[87] Cfr. § 1.

[88] ROMANO, *La legittimazione delle norme penali*, cit., 39, 43.

[89] MUSCO, *Bene giuridico e tutela dell'onore*, Milano, 1974, 85.

[90] A tal proposito vi è in dottrina chi auspica a una «sistematica collaborazione professionale, stabile e istituzionalizzata, fra penalisti ed esponenti delle scienze sociali, in vista di obiettivi di riforma della legislazione penale». FIANDACA, *Sul bene giuridico*, cit., 37. Sulla stessa linea si pone chi sottolinea, con riferimento al bene giuridico, «la consapevolezza di non poter prescindere da una sua ricostruzione anche su base fenomenologica, con la necessità quindi di aprirsi agli apporti di indagini empirico-criminologiche». FORTI, *L'ordinamento lessicale dei beni giuridici*, cit., 375. Ancora, è stato osservato come il concetto di bene giuridico apra «alla considerazione di esigenze concrete, con una forte attenzione al dato empirico», mettendo «in evidenza i legami tra diritto penale e cultura, tra diritto penale e la realtà sociale nelle sue varie componenti», il che dimostra «in modo inequivocabile che il dibattito sul bene giuridico (...) non appartiene soltanto alla dommatica e alla scienza del diritto penale (...), ma è caratterizzato dalla sua apertura ai rapporti della vita reale, alla empiria e alla politica criminale». MERLI, *Introduzione alla teoria generale del bene giuridico*, cit., 26-27.

[91] FORTI, *L'ordinamento lessicale dei beni giuridici*, cit., 374.

La riforma dell'art. 615-*ter* c.p. si pone nel solco dell'imprescindibile adeguamento del sistema penale ai bisogni di tutela connessi alla cd. «vulnerabilità informatica» della società moderna, riconducibile, da una parte, all'incessante digitalizzazione dei servizi, delle attività quotidiane e delle relazioni interpersonali, ulteriormente accelerata dalla pandemia, e, dall'altra, alla diffusione di nuovi fenomeni criminosi che si caratterizzano per modalità di offesa che sfruttano le nuove tecnologie informatiche[92]. In particolare, la norma mira nella sua formulazione attuale e, a maggior ragione, dovrebbe mirare in una sua eventuale versione riformata a prevenire e contrastare gli accessi non autorizzati a un sistema informatico, inteso come entità che, come è stato sottolineato, «nell'era dell'interconnessione e della comunicazione globale, nonché dell'accessibilità e della fruibilità delle risorse attraverso la rete e qualsiasi strumento di comunicazione mobile», «è passato da una dimensione privata o singola a una "dimensione pubblica"»[93]. Pertanto, il bisogno di tutela che legittima la norma e che deve guidare il legislatore in sede di riforma e gli interpreti in sede applicativa ha natura superindividuale, riflettendo l'interesse generale a che l'accesso a dispositivi informatici e spazi virtuali, quanto meno a quelli presidiati da misure di protezione, avvenga lecitamente e in modo da garantire la sicurezza del *cyberspace*. Alla necessità di tutelare l'interesse del singolo alla riservatezza e all'inviolabilità dei *suoi* sistemi telematici, con la progressiva digitalizzazione dei servizi e delle relazioni personali e professionali, si è via via affiancata l'esigenza di proteggere un interesse, quello al regolare accesso ad applicativi informatici e luoghi della rete, che, in quanto «*pre-*

[92] «La vulnerabilità tecnologica della società moderna, connotata dall'inarrestabile evoluzione-rivoluzione informatica e telematica – non solo nei rapporti personali, ma anche in quelli economici, politici, sociali e di rilievo giuridico in genere – è in gran parte dovuta a fenomeni criminosi caratterizzati da nuove modalità di offesa, che sfruttano proprio le potenzialità offerte dalle *Information and Communication Technologies* (ICTs)». FLOR, Voce "*Riservatezza informatica*", in *Diritto on line Treccani - Approfondimenti enciclopedici*, 2017, *www.treccani.it*.

[93] *Ibidem*. Continua l'Autore: «da un lato, è innegabile che una componente di tale "area riservata" riguardi la facoltà, il potere, il diritto del titolare di gestire in modo autonomo le utilità e le risorse del sistema informatico, nonché i contenuti delle comunicazioni informatiche (o telematiche), indipendentemente dalla loro natura», dall'altro, occorre tenere in debita considerazione «le esigenze connesse alla "sicurezza informatica"».

supposto di esercizio virtuale di altri diritti individuali e collettivi»[94] dovrebbe essere inquadrato nella categoria degli interessi diffusi, ossia delle necessità tangibili che fanno a capo alla maggior parte della popolazione[95].
Orbene, il termine "riservatezza", pur associato all'aggettivo "informatica", non pare la scelta terminologica più appropriata a cogliere la nuova dimensione del bene giuridico da proteggere e a orientare l'interprete nella direzione descritta poiché tende a richiamare istanze irriducibilmente individualistiche. Per contro, è possibile prospettare casi di accesso non autorizzato in cui non ricorrono effettive o immediate esigenze di tutela della riservatezza. Si pensi a banche dati, servizi a pagamento o siti destinati a iscritti o abbonati, il cui titolare ha un interesse per lo più economico ad escludere accessi non autorizzati, o all'incriminazione dell'accesso e della permanenza non autorizzati in sistemi istituzionali o di interesse pubblico che, in taluni casi, prima e più che a istanze di tutela della riservatezza, può essere ricondotta alla necessità di garantire la sicurezza di detti sistemi quale riflesso del buon andamento della Pubblica Amministrazione. Ancora, sempre a titolo di esempio, accedere o mantenersi in account o profili pubblici (come quelli di brand o *influencer*) non pare produrre un particolare pericolo per la riservatezza, dal momento che i contenuti sono già pubblici, ma la condotta appare ugualmente meritevole di rimprovero in quanto in contrasto con l'interesse diffuso alla sicurezza e all'esclusività dei sistemi informatici presidiati da misure di sicurezza[96].

---

[94] Così, con riferimento alla *privacy*, MORALES PRATS, *Presupposti politico-criminali per una tutela penale della riservatezza informatica (con particolare riguardo all'ordinamento spagnolo)*, in *Dir. inform.*, 1986, 371 ss.

[95] Si è assistito a un «un percorso di evoluzione della tutela che va dal particolare al generale» simile a quello che ha caratterizzato la manipolazione del mercato e l'*insider trading*, che è partito «dalla dimensione del patrimonio individuale» per arrivare «a quella del risparmio collettivo». Anche a tale proposito si è parlato di un bene che «postula il riferimento» a un «interesse diffuso», in quel caso l'interesse «caratteristico di ogni investitore presente sul mercato a che le proprie scelte possano svolgersi in un contesto di efficienza economica». D'ALESSANDRO, *Regolatori del mercato,* enforcement *e sistema penale*, Torino, 2014, 72.

[96] In dottrina viene evidenziato come la norma tuteli l'«interesse all'esclusività e sicurezza della fruizione e dell'accesso a uno o più spazi virtuali, anche se questi sono "vuoti" o contengono soltanto dati, informazioni e programmi di pubblico dominio». SALVADORI, *I reati contro la riservatezza informatica*, cit., 663-664.

La giurisprudenza di legittimità ha precisato in più occasioni che l'art. 615-*ter* c.p. non mira solo a garantire il diritto alla riservatezza del titolare in ordine a quanto contenuto nel sistema informatico o telematico, bensì la sua personalità in tutte le possibili esplicazioni, comprese quelle di carattere economico-patrimoniale[97]. Viene inoltre enfatizzato in dottrina come non vadano esclusi «dall'ambito della tutela penale quei sistemi informatici e telematici privi di qualsivoglia contenuto personalistico o privatistico», come «i sistemi informatici industriali o commerciali o che gestiscono cataloghi bibliografici o informazioni per il pubblico (es. orari dei treni o appuntamenti culturali), i cui dati vengono trattati solo per finalità di tipo scientifico o culturale o per fornire determinati servizi agli utenti»[98].

Si potrebbe allora pensare a un bene giuridico che costituisca, da una parte, "comune denominatore" dei reati informatici in "senso stretto" e, dall'altra, l'oggetto di tutela "diretta" dell'art. 615-*ter* c.p., quale fattispecie prodromica all'eventuale commissione di altri reati contro la riservatezza o l'integrità di dati e programmi. Un bene che, già nella sua *dimensione semantico-letterale*, denoti una portata ampia e del tutto svincolata dal concetto di riservatezza, come l'*intangibilità informatica*[99], l'*inviolabilità informatica* o l'*intangibilità/inviolabilità dei domini informatici* o *delle sfere virtuali*[100]. Si tratterebbe di un bene giuridico non molto distante quanto a contenuti dalle definizioni di "riservatezza informatica" fornite dalla dottrina; un bene emancipato da quella dimensione fisica, materiale dell'offesa che, indissolubilmente

[97] Cass., Sez. V, 8 maggio 2012, cit. La norma, posta a tutela del domicilio informatico, «non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello *ius excludendi alios*, quale che sia il contenuto dei dati racchiusi in esso, purché attinenti alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati, sia che titolare dello *ius excludendi* sia persona fisica, persona giuridica, privata o pubblica, o altro ente». Cass., Sez. V, 15 febbraio 2021, G.A., in *Diritto e Giustizia*, 2021, 28 aprile.

[98] SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico*, cit., 148.

[99] In questi termini MILITELLO, *Nuove esigenze di tutela penale*, cit., 373 ss. (ripreso da VITARELLI, *Vita privata nel diritto penale*, in *Dig. disc. pen.*, XV, Torino, 1999, 310 e da PIERGALLINI, *I delitti contro la riservatezza informatica (artt. 615*-ter*, 615*-quater*, 615*-quinquies), cit., 774).

[100] Si è osservato come l'art. 615-*ter* c.p. sia volto a garantire «l'interesse al godimento esclusivo, sicuro e indisturbato degli "spazi" informatici o *sfere virtuali*». SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico*, cit., 157 (corsivo nostro).

legata al concetto di "domicilio", non riproduce fedelmente la realtà della criminalità informatica; un bene che, grazie alla sua formulazione ampia e "neutrale", potrebbe *meglio orientare l'interpretazione* della norma e vantare una certa *resilienza* e *versatilità* rispetto alla costante evoluzione della fenomenologia e della casistica delle offese informatiche.

La locuzione "intangibilità informatica", ad esempio, è stata ritenuta idonea a manifestare «la multiforme esigenza di non alterare la relazione triadica fra dato della realtà, rispettiva informazione e soggetti legittimati a elaborare quest'ultima nelle sue diverse fasi (creazione, trasferimento, ricezione)», relazione che talvolta (ma non sempre) può assumere un valore economico. Tale interesse potrebbe pertanto operare quale «criterio orientativo per una razionale politica criminale, al fine di sviluppare [o riformare] una apposita normativa incriminatrice nella duplice prospettiva offerta dai canoni di sussidiarietà e proporzione». Ancora, esprimendo «in termini generali l'essenza dell'offesa realizzata nella categoria dei reati informatici può contribuire a evitare il rischio di soluzioni incriminatrici troppo ancorate ai caratteri specifici dei mezzi informatici di un particolare "stato dell'arte"»[101]. Mentre una nozione più ristretta e, in quanto tale, linguisticamente più precisa di "riservatezza informatica", potrebbe essere utilizzata per indicare, «in un'ottica di "seriazione" degli interessi da tutelare»[102], uno dei beni eventualmente e indirettamente protetti dall'art. 615-*ter* c.p., nonché il precipuo oggetto di tutela di altre fattispecie[103].

Gli stessi Autori della proposta di riforma evidenziano come «le categorizzazioni» abbiano «un'attitudine esplicativa comunque limitata» e come spetti «al legislatore definire un'area di offesa tipica riferita alle diverse sottocategorie e anche alle singole fattispecie, tale da consentire all'interprete di individuare e

[101] MILITELLO, *Nuove esigenze di tutela penale*, cit., 373 ss.

[102] MANNA, *Prime osservazioni sul Testo Unico in materia di protezione dei dati personali: profili penalistici*, in *www.privacy.it* (2003), 1125 ss.

[103] Si tratterebbe quindi di invertire la logica secondo la quale l'art. 615-*ter* c.p. tutelerebbe in via diretta lo «*ius excludendi alios* del titolare del sistema» e «indirettamente anche l'interesse collettivo al regolare funzionamento, alla integrità e alla disponibilità dei sistemi». Così SALVADORI, *I reati contro la riservatezza informatica*, cit., 664.

praticare le corrette opzioni interpretativo-applicative nella fase della sussunzione del fatto concreto nel tipo astratto»[104].

Proprio per la sua portata non strettamente individuale e privata, il bene giuridico tutelato dalle norme in materia di trattamento dei dati personali non viene individuato dalla Corte di Giustizia dell'Unione europea nella riservatezza (o, secondo la terminologia anglosassone, nella *privacy*), bensì nel diritto alla protezione dei dati personali, quale *diritto del singolo* e *interesse della collettività*. La disciplina del trattamento dei dati personali si rivela infatti «irriducibile alla sola cifra individualistica»[105], andando oltre la sfera privata e finendo per attingere le garanzie di trasparenza e legalità quali presupposti del funzionamento del sistema democratico[106]. Allo stesso modo, l'interesse a impedire accessi non autorizzati a sistemi informatici pare esulare dalla dimensione strettamente soggettiva riflettendo istanze di natura superindividuale – fra cui l'intangibilità, l'utilizzo indisturbato, la disponibilità e la sicurezza dei sistemi informatici – che sarebbe bene mettere in evidenza già nella *dimensione semantico-lessicale* dell'interesse protetto, conferendogli in questo modo, fra l'altro, una maggiore *capacità di adattamento* rispetto a futuri profili di "vulnerabilità informatica", senza per questo aprire la strada a interpretazioni analogiche in *malam partem*[107]. Del resto, non mancano in dottrina prospettive tese a enfatizzare la valenza *assiologica* delle scelte lessicali e lo stretto legame fra opzioni linguistiche e pregnanza concettuale della produzione normativa[108]. Così, anche da una denominazione più appropriata del bene giuri-

[104] FIORE, *Proposta di riforma*, cit., 3.

[105] RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, 19 ss., 101 ss.

[106] In una società sempre più globalizzata e "connessa", l'evoluzione normativa scaturita dall'esigenza di tutelare la *privacy* quale prerogativa individuale ha progressivamente coinvolto interessi di portata generale attribuendo un ruolo centrale alla protezione dei dati personali che, in forza del nuovo Regolamento 2016/679/UE, ha assunto la connotazione ulteriore di «diritto pubblico europeo». PIZZETTI, *La protezione dei dati personali dalla direttiva al nuovo regolamento: una sfida per le Autorità di controllo e una difesa per la libertà dei moderni*, in *Rivista del diritto dei media*, 2018, 1, 10.

[107] Sul *discrimen* fra interpretazione analogica e interpretazione estensiva, evolutiva e teleologica si veda FIANDACA, MUSCO, *Diritto penale. Parte Generale*, cit., 121 ss., 127 ss.

[108] FORTI, *L'ordinamento lessicale dei beni giuridici*, cit., 361 ss. Cfr. MANNOZZI, *Le parole del diritto penale: un percorso ricostruttivo tra linguaggio per immagini e lingua giuridica*, in *Riv. it. dir. proc. pen.*, 2011, 1431 ss.; DE MAGLIE, *La lingua del diritto penale*, in *Criminalia*, 2018, 105 ss. ove si rileva la necessità di respingere «con risolutezza» le ambiguità connesse alla «condizione di "polisemia

dico di volta in volta tutelato, che tenga conto del suo operare quale «strumento principale per comprendere l'essenza e il contenuto del reato»[109], dipende quella funzione *promozionale* e di *orientamento culturale* che, unitamente alla funzione di controllo sociale, viene attribuita al diritto penale[110].

8. *Conclusioni: il diritto penale dell'informatica fra proporzione e "logiche piramidali".* La teoria del bene giuridico e l'accennato parallelismo fra protezione dei dati personali e protezione dei sistemi informatici consentono di sviluppare brevi riflessioni conclusive.

L'individuazione dell'*intangibilità* o *inviolabilità informatica* o *intangibilità/inviolabilità dei domini informatici* o *delle sfere virtuali* quale bene diffuso protetto *in via principale* e *diretta* dall'art. 615-*ter* c.p. – il quale tutelerebbe in via solo *eventuale* e *indiretta* l'interesse del singolo alla riservatezza dei *suoi* sistemi informatici e spazi virtuali – potrebbe garantire una maggior attinenza della fattispecie all'evoluzione recente e futura degli accessi non autorizzati che – come enfatizzato dagli stessi proponenti della riforma – riguardano anche i sistemi «privi di qualsivoglia contenuto personalistico o privatistico»[111]. Un siffatto bene giuridico potrebbe quindi svolgere sia una funzione *interpretativa*, vale a dire di «filo conduttore per l'interpretazione»[112] e l'applicazione della norma e, in particolare, di collegamento del diritto penale alla realtà empirico-sociale, sia una funzione *sistematica* (o *classificatoria*), nel senso di stimolare la riflessione sull'opportunità di mantenere tale fattispecie e quelle che seguono nella Sezione III del Capo III del Libro XII, dedicata ai delitti

dell'espressione linguistica"» e di osteggiare le situazioni di «opacità linguistico-normativa», in quanto la legittimazione del diritto penale passa anche attraverso il suo modo di comunicare. «La chiarezza della lingua del diritto penale rappresenta una garanzia irrinunciabile di democrazia nel sistema. Infatti la "democrazia vive di parole precise". Ciò significa che l'accessibilità e la trasparenza del linguaggio penalistico sono un presupposto irrinunciabile perché sia rispettato il principio di uguaglianza». *Ivi*, 31. Cfr. CAROFIGLIO, *Con parole precise. Breviario di scrittura civile*, Bari, 2015, 41 ss.

[109] MERLI, *Introduzione alla teoria generale del bene giuridico*, cit., 19.

[110] In proposito si veda BOBBIO, *Dalla struttura alla funzione. Nuovi studi di teoria del diritto*, Milano, 1977, 13 ss. Sull'attitudine del diritto penale «a stimolare e consolidare regole sociali, prepenalistiche» si veda FORTI, *Principio del danno e legittimazione "personalistica" della tutela penale*, cit., 80 ss.

[111] SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico*, cit., 148.

[112] MUSCO, *Bene giuridico e tutela dell'onore*, cit., 85.

contro la libertà morale, piuttosto che creare un capo o una sezione a sé, dedicati proprio ai delitti contro l'intangibilità o inviolabilità informatica, in cui far eventualmente confluire anche i reati in materia di trattamento dei dati personali, in relazione ai quali in dottrina taluno ha invocato la cd. riserva di codice[113].

Nondimeno, le conseguenze che potrebbero derivare sul piano interpretativo e applicativo dall'identificazione di tale interesse protetto non operano nel senso di delimitare, ma semmai di ampliare l'ambito del punibile, offuscando quella funzione *critico-selettiva* storicamente attribuita alla categoria del bene giuridico. La fattispecie, stando alla configurazione descritta, si applicherebbe – come peraltro già avviene – a prescindere dall'offesa a un interesse del singolo o a un rilevante interesse pubblico, essendo sufficiente l'offesa all'interesse diffuso all'*intangibilità/inviolabilità* dei sistemi informatici, offesa immanente agli accessi non autorizzati, incentrandosi il disvalore oggettivo e soggettivo della condotta nella violazione delle disposizioni del titolare, talvolta chiaramente desumibili solo dalle misure di sicurezza poste a protezione del sistema, che, per questa ragione, si ritiene opportuno conservare quale elemento di fattispecie[114].

L'attribuzione della nuova veste lessicale e – potenzialmente – di nuove sfumature semantiche – al bene giuridico invita dunque a domandarsi, prevenendo plausibili rilievi critici, se il ricorso al diritto penale e, a maggior ragione, a una pena che può arrivare, già nell'ipotesi base, a tre anni di reclusione, sia giustificato alla luce dei principi di *extrema ratio* e proporzionalità del di-

[113] Sull'«occasione perduta» di inserire nel codice penale i reati in tema di protezione dei dati personali con il d.gls. 10 agosto 2018, n. 101 di adeguamento del nostro ordinamento al GDPR, dando così attuazione alla cd. "riserva di codice", si veda BRIZZI, *Privacy. La tutela penale dei dati personali*, Milano, 2020, 33 ss. Cfr. sul punto anche TRONCONE, *La tutela penale della riservatezza e dei dati personali. Profili dommatici e nuovi approdi normativi*, cit., 31 ss. In tema di riserva di codice, *inter alios*, DONINI, *La riserva di codice (art. 3-bis Cp) tra democrazia normante e principi costituzionali. Apertura di un dibattito*, in *Leg. pen.*, 2018, 1 ss.; PALIERO, *La "riserva di codice" messa alla prova: deontica idealistica "versus" deontica realistica*, in *Criminalia*, 2019, 31 ss.; ROTOLO, *Riserva di codice e legislazione penale complementare*, in *JusOnline*, 2019, 3, 160 ss.

[114] Riprendendo la già richiamata distinzione fra tutela del "contenitore" e tutela del "contenuto" (PLANTAMURA, *Domicilio e diritto penale*, cit., 187-188) l'ipotesi criminosa tutelerebbe direttamente il "contenitore", che pure non deve essere inteso nell'accezione "fisica" e "materiale" sottesa al concetto di "domicilio", e solo in via indiretta ed eventuale il "contenuto".

ritto penale. Ponendosi in questa prospettiva, la normativa in materia di protezione dei dati personali attribuisce rilevanza penale a condotte che arrecano «nocumento all'interessato»[115] o che, tenute «al fine di recare danno», abbiano per oggetto materiale archivi automatizzati, o una parte sostanziale di essi, contenenti «dati personali oggetto di trattamento su larga scala». Mentre negli altri casi, le condotte di illecito trattamento dei dati sono sanzionate sul piano amministrativo[116]. Il modello definito di *accountability* o *pyramidal enforcement*, che informa in una certa misura il sistema di tutela dei dati personali, si fonda su una "logica scalare" in forza della quale solo qualora falliscano forme di persuasione morale all'osservanza dei precetti si ricorre a strumenti sanzionatori partendo da quelli meno invasivi offerti dal diritto civile e amministrativo per poi, in linea con il principio di *extrema ratio*, ricorrere al diritto penale[117].

Lo stesso approccio "piramidale" potrebbe essere adottato in materia di accesso non autorizzato ad un sistema informatico (secondo la nuova denominazione della fattispecie suggerita dai proponenti), nel senso di riservare la pena detentiva ai casi in cui dalla condotta derivi almeno un pericolo per

---

[115] Se la precedente formulazione della fattispecie di illecito trattamento di dati personali di cui all'art. 167 del Codice della *privacy* suggeriva un inquadramento dogmatico del "nocumento all'interessato" quale condizione obiettiva di punibilità, dopo la riforma del 2018 tale locuzione viene qualificata dagli interpreti quale elemento costitutivo del reato in particolare, come evento), aderendo a una soluzione cui era peraltro già pervenuta in via ermeneutica la stessa giurisprudenza. Sul punto MANES, MAZZACUVA, *GDPR e nuove disposizioni penali del Codice privacy*, in *Dir. pen. proc.*, 2019, 2, 173.

[116] Il riferimento è agli artt. 167, 167-*bis* e 167-*ter* del Codice della *privacy* per quanto concerne le fattispecie incriminatrici e agli artt. 83 e 84 del GDPR in relazione agli illeciti amministrativi. Un recente commento della disciplina si deve a MARTIELLO, *La tutela penale dei dati personali: un'introduzione agli artt. 167, 167-bis e 167-ter del c.d. «codice della privacy»*, in *Discrimen*, 2 marzo 2022.

[117] L'elaborazione di tale modello si deve al Professore australiano ideatore della *restorative justice*, John Braithwaite. BRAITHWAITE, *Restorative Justice and Responsive Regulation*, Oxford, 2002, 29 ss.; AYRES, BRAITHWAITE, *Responsive Regulation: Transcending the Deregulation Debate*, Oxford, 1992, 35 ss.; FISSE, BRAITHWAITE, *Corporations, Crime and Accountability*, Cambridge, 1993, 140 ss. Sul tema anche MAZZUCATO, *Giustizia esemplare. Interlocuzione con il precetto penale e spunti di politica criminale*, in *Studi in onore di Mario Romano*, Napoli, 2011, 408 ss.; DONINI, *Per una concezione post-riparatoria della pena. Contro la pena come raddoppio del male*, in *Riv. it. dir. proc. pen.*, 2013, 1206 ss.; SPRICIGO, *Un approccio "responsivo" per le ipotesi di illecito colposo in ambito medico*, in *Riv. it. med. leg.*, 2014, 107 ss.; ROTOLO, *'Riconoscibilità' del precetto penale e modelli innovativi di tutela. Analisi critica del diritto penale dell'ambiente*, Torino, 2018, 234 ss.

l'interesse del titolare del sistema o per un rilevante interesse pubblico. Mentre la previsione della sola pena pecuniaria o di una sanzione civile o amministrativa parrebbe più adeguata in relazione a quelle condotte che, pur ledendo l'interesse diffuso all'intangibilità o inviolabilità informatica, non si traducano né nell'offesa all'interesse di un singolo né nell'offesa a un rilevante interesse generale[118]. In questa direzione pare timidamente orientarsi anche la proposta di riformulazione della norma in commento laddove prevede una pena aggravata, fra l'altro, in caso di condotte che «riguardano sistemi informatici di pubblica utilità»[119]. Il nostro legislatore, d'altro canto, si è già dimostrato sensibile all'opportunità di esplorare, nel settore in esame, logiche responsive e sanzioni amministrative, anzitutto per la loro idoneità a prevenire e intercettare condotte di accesso non autorizzato imputabili a imprese. Da anni la fattispecie di cui all'art. 615-*ter* c.p. è stata infatti introdotta nel catalogo dei reati presupposto ex d.lgs. 8 giugno 2001, n. 231[120].

---

[118] La fattispecie, così concepita, eviterebbe anche quell'ambigua dimensione plurioffensiva che, come ben evidenziato in dottrina, se non adeguatamente arginata, rischia di tradursi, in sede applicativa, in un'eccessiva dilatazione dell'ambito del punibile, depotenziando ulteriormente la funzione *critico-selettiva* del bene giuridico. Si è infatti assistito a prassi giudiziali in cui la plurioffensività è stata invocata per dissimulare «beni vaghi o sfumati» o è stata intesa come offensività alternativa di un bene giuridico piuttosto che di un altro, portando a condanne per condotte che, in concreto, non avevano offeso né l'uno né l'altro bene. Al contrario, stando all'inquadramento proposto, la fattispecie, di regola, sarebbe *monoffensiva*, ossia volta a tutelare l'interesse superindividuale all'intangibilità informatica e, solo in alcuni casi, puniti più severamente, *virtuosamente plurioffensiva*, ossia tale, secondo la vocazione originaria della categoria della plurioffensività, da intercettare l'offesa simultanea e non alternativa all'interesse del singolo all'inviolabilità dei *suoi* sistemi informatici o un rilevante interesse pubblico (come quello al buon andamento della Pubblica Amministrazione) e a quello diffuso al regolare accesso agli spazi digitali. Cfr. *ex multis*, MANES, *Il principio di offensività nel diritto penale*, cit., 84 ss., ove si sottolinea come «nella prassi applicativa corrente il riferimento ad oggetti di tutela vaghi o sfumati (...) venga spesso diluito e stemperato attraverso lo schema, comodo quanto inappagante, della "plurioffensività", nel tentativo di imbellettarne la portata onnivora, ma con l'unico risultato di pregiudicare ulteriormente il contenuto garantistico e la capacità critica del bene giuridico (e, simmetricamente, del principio di necessaria lesività)»; EUSEBI, *L'insostenibile leggerezza del testo. La responsabilità perduta della progettazione politico-criminale*, in *Riv. it. dir. proc. pen.*, 2016, 1675, ove vengono censurate «letture dilatative della sfera di applicabilità dell'illecito», spesso originate dalla «facilità con cui s'è *teorizzato*, fino a oggi, il carattere *plurioffensivo* di non pochi reati».

[119] PICOTTI, FLOR, SALVADORI, Proposta di riforma dei *Reati contro l'inviolabilità del domicilio, la tutela della vita privata e dei segreti, la libertà e la personalità informatica*, cit., 10.

[120] Art. 24-*bis* (Delitti informatici e trattamento illecito di dati), introdotto dalla l. 18 marzo 2008, n. 48.

Un simile ripensamento della disciplina dell'accesso non autorizzato a sistema informatico pare riflettere al meglio il principio di *proporzione* come descritto dalla dottrina penalistica, vale a dire come principio che «si specifica in campo penale nella proposizione per cui una reazione per essere legittima deve essere proporzionata alla condotta offensiva»[121], dipendendo il disvalore di quest'ultima anche dalla sua incidenza, almeno in termini di pericolo concreto, su beni strettamente personali o di spiccata rilevanza pubblica. Verrebbe così enucleata un'ulteriore funzione che può essere riconosciuta alla categoria del bene giuridico, una funzione strettamente connessa al principio di proporzione e che consiste nell'orientare la *modulazione* della risposta penale (ed extrapenale). In altri termini, l'attribuzione all'interesse protetto di una dimensione linguistica più precisa e "realistica", che consenta di cogliere l'ampia casistica sottesa all'incriminazione, stimola la riflessione, in una logica *de iure condendo*, o meglio "*de iure reformando*", non solo sulla collocazione sistematica della norma, ma altresì sulla graduazione della risposta sanzionatoria.

D'altronde, individuare equilibri sempre nuovi fra diritti e libertà nel *cyberspace*, monitorando l'incessante evoluzione della fenomenologia delle offese che vi vengono perpetrate, è una delle principali sfide che chi si occupa di diritto penale dell'informatica è oggi chiamato ad affrontare, nel tentativo di preservare e rafforzare il ruolo della tecnologia digitale quale «fattore di *coesione della società civile e delle sue libertà*»[122].

---

[121] DEMURO, Ultima ratio: *alla ricerca di limiti all'espansione del diritto penale*, in *Riv. it. dir. proc. pen.*, 2013, 1660. Continua l'Autore: «nella logica costi-benefici, il principio esprime l'esigenza che i vantaggi che la società si attende dalla comminatoria penale (prevenzione di fatti socialmente dannosi) siano idealmente confrontati con i costi immanenti alla pena in termini sociali, economici e individuali, di sacrificio per i beni della libertà personale, del patrimonio, dell'onore, ecc.». In tema di proporzione della pena si veda anche PALIERO, *Il Mercato della Penalità*, cit., ove viene messa in rilievo la complessità di un'equazione fra grandezze eterogenee quali la *qualità*, in termini di *gravità*, del reato e la *quantità*, o meglio la *misura*, della pena. *Ivi*, 1.

[122] Già negli anni Ottanta l'informatica veniva descritta come «fenomeno di massa» e si osservava come, «paradossalmente», essa potesse «essere utilizzata come nuova forma di *totalitarismo virtuale* oppure come un nuovissimo fattore di *coesione della società civile e delle sue libertà*». Opzione quest'ultima che doveva all'epoca e deve ancora oggi «stimolare ad affrontare lo studio dello sviluppo informatico allo scopo di chiarire quali sono le *libertà tecnologiche* dell'individuo e quali le condizioni che ne possono permettere l'uso». MORALES PRATS, *Presupposti politico-criminali per una tutela penale della*

riservatezza informatica, cit., 369-371.