FILIPPO BERTO

Recensione a Cybercrime *e tutela penale del patrimonio*, C. Crescioli, Milano, 2024, pp. XXI-442

Recensione al volume *Cybercrime e tutela penale del patrimonio.*

Review of Cybercrime e tutela penale del patrimonio, C. Crescioli, Milan, 2024, pp. XXI-442.

Review of the book Cybercrime e tutela penale del patrimonio.

Lo sviluppo delle tecnologie e dei sistemi informatici e telematici ha apportato indubbi benefici al traffico giuridico e una crescente semplificazione degli scambi commerciali. Tuttavia, come noto, all'evoluzione del cd. *cyberspace* e delle potenzialità che esso ha prodotto si accompagna, di pari passo, l'adattamento dei fenomeni criminali, i quali costituiscono, proprio per la loro raffinatezza, una sfida per la tutela dei beni fondamentali dell'individuo e per la sicurezza dello Stato. Invero, vittime dei reati commessi nel mondo virtuale sono gli individui, in quanto portatori di beni giuridici fondamentali, così come le infrastrutture statuali, che sono sempre più colpite da operazioni illecite transfrontaliere, finalizzate alla destabilizzazione del tessuto economico e sociale.
Al tempo stesso, l'evoluzione tecnologica della criminalità e, di conseguenza, degli strumenti congeniati per contrastarla, rappresentano una sfida per la tenuta delle categorie classiche del diritto penale, concepito come strumento di tutela dei beni giuridici, tra cui figura, nelle sue diverse concezioni, il patrimonio. La sfida per gli ordinamenti contemporanei è, dunque, adeguare la risposta penale nella prospettiva dell'efficacia della tutela, pur tuttavia senza uscire dal perimetro segnato dai principi fondanti il diritto penale liberale.
Entro tale contesto si inserisce la monografia Cybercrime *e tutela penale del patrimonio. Un'indagine in prospettiva comparata*, che costituisce l'esito del triennio di ricerca dottorale della dott.ssa Chiara Crescioli.
La presente opera ha il pregio di fornire un'ampia disamina delle rilevanti dinamiche criminologiche che governano il cyberspazio, a cui segue una organica analisi dell'impatto dell'introduzione dei nuovi reati informartici sulle categorie

tradizionali dell'ordinamento penale interno e, prima ancora, eurounitario. È stato così puntualmente ripercorso lo sviluppo diacronico della legislazione sovranazionale e nazionale in tema; a tal fine, efficace risulta l'assetto della trattazione delle singole fattispecie, suddivise in tre macrocategorie: reati preparatori, reati *lato sensu* patrimoniali e fenomeni di reimpiego del denaro proveniente da delitto.

Inoltre, la lineare e completa trattazione tesa ad evidenziare le principali criticità del sistema normativo oggi in vigore non rinuncia a delineare una *pars construens*, nella quale emerge l'impegno dell'Autrice a proporre diverse soluzioni interpretative alle questioni ancora discusse nella legislazione vigente. A queste ultime si accompagnano ambiziose proposte di ripensamento del sistema, vagliate tutte in modo critico e con un approccio realistico, attento alla vita applicativa del diritto penale e agli sviluppi del diritto ventura. Ad arricchire tali riflessioni contribuisce in modo sostanziale l'analisi di diritto comparato, il quale lungi dall'essere una mera ricognizione delle analogie e delle asimmetrie normative tra diversi sistemi. Anzi, la ricerca di un ragionato confronto con la legislazione spagnola e tedesca è risultata essere la chiave imprescindibile per svolgere delle considerazioni generali sull'idoneità del diritto eurounitario a fungere da strumento di armonizzazione degli ordinamenti nazionali e implementazione degli *standard* di tutela del bene-patrimonio.

Il primo capitolo esordisce con l'affermazione della meritevolezza di tutela del patrimonio e della conseguente necessità di attivare la risposta penale a fronte delle condotte che offendono il patrimonio. A fondamento di tale assunto e al fine di fornire un fondamento teorico-dogmatico utile a comprenderne la portata, vengono ripercorse le "concezioni penalistiche" con cui tradizionalmente si definisce il patrimonio: a quella economica si contrappongono quella giuridica e giuridico-funzionale. Tuttavia, l'adozione dell'una o dell'altra concezione, tutte oggetto di numerose critiche mosse dalla più autorevole dottrina, non cambia la conclusione a cui unanimemente si giunge osservando il tratto

comune dei reati contro il patrimonio, così come diffusamente disciplinati nel Codice penale; questo, infatti, coincide con la natura patrimoniale degli interessi giuridici lesi. In altre parole, tali fattispecie tutelano il diritto soggettivo che ha ad oggetto il rapporto di signoria di un individuo su un "cosa", dove con quest'ultima l'Autrice si riferisce ad "ogni entità materiale del mondo esteriore diversa dall'uomo, avente la capacità strumentale a soddisfare un bisogno umano, materiale o spirituale".

Fornito un quadro complessivo della nozione di patrimonio, ne viene sottolineata la dinamicità; caratteristica, quest'ultima, che consente di estenderne la portata anche alla crescente diffusione di oggetti dematerializzati o immateriali. Nondimeno, una tale dilatazione dell'ambito applicativo del patrimonio è stata il frutto di interventi legislativi e giurisprudenziali, sconfinati finanche, a giudizio dell'Autrice, in vere e proprie interpretazioni estensive, se non persino analogiche, della nozione di "cosa". Punto fermo rimane, in ogni caso, la natura di diritto soggettivo, che, seppur di natura non primaria, è funzionale alla tutela di beni costituzionali, quale lo sviluppo della persona. Invero, nella trattazione viene a più riprese sottolineato come le nuove forme di aggressione del patrimonio nel cyberspazio ledano, in realtà, una pluralità di beni giuridici; primo tra tutti, la riservatezza informatica, tutelata quale spazio dove esercitare facoltà in modo libero e comunicare senza interferenze. Ad esempio, una condotta illecita che si estrinseca in un pagamento (o nell'intercettazione di un pagamento) *online* non può prescindere dal previo ottenimento di dati personali o dall'accesso al sistema informatico altrui di cui all'art. 615-*ter* c.p., ossia da singole azioni funzionalmente connesse alla successiva operazione lesiva del patrimonio del titolare dei dati.

Altri sono gli interessi che vengono in gioco, sebbene a loro volta funzionali alla tutela della riservatezza informatica: l'identità digitale e l'integrità e la sicurezza informatica, in particolare nel caso di attacco cibernetico operato tramite strumenti tecnologici, quali i *malware*. E ancora, nelle ipotesi di furto di identità

virtuale e di occultamento delle somme ricavate con i suddetti reati, così come nel caso di danneggiamento rivolto a sistemi informatici pubblici, vengono in rilievo beni di respiro superindividuale, come l'ordine pubblico economico, l'amministrazione della giustizia e la pubblica fede.

Prima di addentrarsi nell'analisi strettamente giuridica, l'Opera presenta una ricca disamina dei nuovi metodi di pagamento diversi dal denaro e delle peculiari dinamiche illecite che si sviluppano nel *web*. Viene, quindi, fornito il substrato tecnico a cui ancorare il contenuto dei singoli reati.

Tra gli innovativi mezzi di pagamento spiccano, per attualità e problematicità applicativa, le criptovalute e i *token*, spesso utilizzati nelle pratiche illecite, potendo garantire maggiore garanzia di anonimato, oltre ad essere talvolta oggetto delle stesse condotte criminose. Quanto invece alla sfera applicativa dei nuovi fenomeni criminosi, risulta oggi di tutta evidenza come i cybercriminali, spesso parte di organizzazioni criminali, anche transfrontaliere e aventi struttura peculiare rispetto alle associazioni criminali comuni (si pensi al ruolo dei cd. *money mules*), sfruttino le tecnologie e, *in primis*, l'intelligenza artificiale; quest'ultima, infatti, funge da strumento funzionale ad una maggiore personalizzazione dei messaggi truffaldini, ad individuare la vulnerabilità di un particolare sistema informatico e, infine, a sfuggire ai controlli di altri sistemi che utilizzano a loro volta l'IA.

In merito agli schemi criminosi all'interno dei quali vanno inserite le diverse fattispecie criminose, deve essere segnalato il cd. *Cybercrime-as-a-service*, vero e proprio modello a cui devono essere ricondotte molte delle pratiche illecite riscontrabili nel cyberspazio: alcuni soggetti offrono la "merce" – ossia credenziali e dati personali delle vittime e *software* maligni – nei mercati illegali che proliferano nel *dark web*, dove poi questa verrà venduta a soggetti che, in un secondo momento, si renderanno responsabili di ulteriori reati contro il patrimonio. Come risulta evidente, le diverse operazioni lesive non sono atomi a sé stanti, ma costituiscono uno schema articolato di operazioni criminali.

In tale ambito, suscitano particolare interesse le pratiche criminose che rappresentano la trasposizione nel mondo virtuale delle azioni decettive ed estorsive tradizionali, ossia le truffe *online*, gli schemi Ponzi, le *advanced fee fraud*, la *cyber extortion* e *sextortion* e i danneggiamenti informatici. Altrettanto rilevanti sono le pratiche di *social engineering* impiegate per realizzare i *cybercrimes* più disparati, tra le quali ricopre un ruolo indubbiamente preminente il *phishing*, ormai diffuso in diverse varianti.

Nell'analisi delle diverse dinamiche criminologiche l'Autrice adotta la prospettiva della persona offesa e, una volta riaffermata la necessità di garantire alla stessa una tutela efficace, segnala le peculiari tendenze alla (auto)colpevolizzazione delle vittime coinvolte nelle truffe *online*. Tale rilievo emerge tanto più se si considera che in molte delle fattispecie criminose che vengono commesse nel cyberspazio – non solo quelle riconducibili a schemi fraudolenti – la vittima assume un inconsapevole ruolo attivo nella realizzazione dell'illecito. Proprio a partire da tale ultima considerazione, viene svolta una fondamentale riflessione circa l'inattualità della tradizionale ripartizione dei reati contro il patrimonio contenuta nel Codice Rocco: il *discrimen*, che tradizionalmente si fondava sull'accertamento della cooperazione artificiosa della persona offesa, è quindi ora messo in crisi dalla promiscuità dei contributi causali dei soggetti attivo e passivo. Si pensi alla prima fase dell'illecito, dove il reo riesce a carpire le informazioni proprio grazie ad una condotta collaborativa dell'ignaro soggetto passivo, mentre nella seconda fase, caratterizzata dall'illecita sottrazione e dal conseguente depauperamento, è assente il coinvolgimento attivo della vittima. In definitiva, grazie all'utilizzo di strumenti informatici sofisticati, le condotte che, nel loro sviluppo iniziale, rientrerebbero negli schemi fraudolenti a cooperazione della vittima hanno, nella fase dell'esecuzione, maggiori affinità con il paradigma della sottrazione unilaterale, ponendosi in una zona grigia tra il modello del furto e quello della truffa. Conseguentemente, anche la differenziazione del trattamento sanzionatorio, che tradizionalmente punisce più

gravemente i reati ad offesa unilaterale, merita di essere ripensato: non appare opportuno, infatti, irrogare una pena maggiore al soggetto resosi responsabile di furto, rispetto a quello che ha commesso una frode informatica; scelta che verrebbe aprioristicamente fondata sulla mera constatazione per cui l'azione dell'*hacker* risulterebbe agevolata dalla condotta del soggetto passivo.

Abbandonata l'ampia ed esaustiva esposizione delle nozioni giuridiche e criminologiche istituzionali, l'Opera fornisce una ricognizione dell'evoluzione della normativa internazionale e sovranazionale in tema, a partire dalla Convenzione *Cybercrime* del 2001, approvata in seno al Consiglio d'Europa e sottoscritta altresì da Stati non appartenenti a tale organizzazione internazionale, sino alle più recenti direttive 2013/40/UE e 2019/713/UE. Proprio le considerazioni sulla legislazione europea in materia di contrasto ai reati cibernetici risultano il perno su cui ruotano le riflessioni centrali della trattazione; invero, tema ricorrente dell'opera monografica è lo studio delle relazioni tra la disciplina interna e quella sovranazionale. L'obiettivo finale è, dunque, verificare l'eventuale raggiungimento degli *standard* di tutela e di armonizzazione normativa che il legislatore europeo si è prefissato.

La monografia entra così nel vivo dell'analisi tecnico-penalistica, condotta attraverso lo studio delle singole fattispecie di reato. La ricerca si concentra così, in primo luogo, sugli atti preparatori alla commissione dei reati strettamente patrimoniali; categoria per la verità piuttosto ampia, all'interno della quale vi rientrano fattispecie di particolare rilevanza applicativa e diverse per struttura e beni protetti.

Condivisibile è il giudizio positivo dell'Autrice per la scelta di politica-normativa seguita dal legislatore, il quale ha inserito le nuove fattispecie a fianco a quelle previgenti, seguendo il criterio del bene giuridico leso. A ben vedere, infatti, la tipizzazione di tali reati risulta strumentale alla tutela dei beni giuridici protetti dalle fattispecie tradizionali.

Maggiormente problematica è l'inevitabile frizione che l'anticipazione della

tutela del patrimonio provoca nei confronti dei principi di proporzionalità, sussidiarietà e frammentarietà. Invero, ciò che viene censurato è il ricorso alla scure della pena per quelle condotte che non costituiscono una grave aggressione ai beni giuridici tutelati dall'ordinamento. In merito a ciò, si pensi alla punibilità del mero possesso di dati informatici e di *software*, qualificato come atto preparatorio di altri reati commessi con quegli stessi mezzi; proprio in tale ipotesi viene segnalata la natura di per sé neutra della condotta, *a fortiori* se si considera la natura dei *dual-use* dei *software*, che possono dunque essere utilizzati per scopi sia leciti che illeciti. Dunque, il rischio che viene segnalato è che le norme che incriminano gli atti preparatori finiscano per punire condotte di per sé inoffensive. Ovvero, all'opposto, non essendo agevole determinare l'elemento discretivo per determinare se lo strumento informatico pone in pericolo il bene giuridico, le stesse rischiano di essere eccessivamente restrittive e, pertanto, inefficaci. A ciò non giova di certo la tendenza della legislazione sovranazionale ad introdurre veri e propri elenchi di fattispecie da punire, prassi che si scontra con la prospettiva di un diritto penale dell'*extrema ratio*.
Ma l'ipertrofia legislativa non si limita a creare un attrito con i principi di sussidiarietà e frammentarietà: l'introduzione di numerose fattispecie che sembrano *prima facie* disciplinare azioni criminose distinte, produce rilevanti problematiche sul versante applicativo, specialmente per quanto attiene al concorso – reale o apparente – tra più reati applicabili al medesimo fatto storico.
Le riflessioni che l'Autrice, a più riprese, riserva a tale problematica costituiscono un contributo originale e pregevole, data l'attualità della questione nella prassi e i conflitti interpretativi che ne sono sorti. In particolare, l'elemento che solleva maggiori problematicità risulta essere l'orientamento della giurisprudenza di legittimità che ritiene quello di specialità quale unico criterio applicabile al fine di individuare i casi di concorso apparente di reati. Infatti, in molti casi tale criterio non risulta sufficiente ad assurgere a strumento regolativo del rapporto tra reati. Inoltre, va specificato che in un campo come quello di cui

trattasi sono molte le condotte tra loro interdipendenti e facenti parte di una medesima progressione criminosa. È evidente, quindi, che l'applicazione del regime del reato continuato rischia di tradursi in un *vulnus* al principio di proporzionalità.

Pertanto, l'Autrice sonda l'applicabilità del diverso criterio di consunzione-assorbimento, maggiormente idoneo a disciplinare il rapporto tra reati. Tuttavia, lo stesso, per evitare i profili di irragionevolezza prodotti dal confronto tra fattispecie astratte, andrebbe ancorato alla sola "dimensione concreta del fatto".

Seguendo il già evidenziato schema logico, l'Opera prosegue con la disamina dei reati cd. *lato sensu* patrimoniali, i quali si pongono su di un piano concettuale e cronologico successivo rispetto a quelli analizzati in precedenza. Tra le fattispecie che appartengono a questa categoria vi sono la truffa *online*, nella sua eventuale forma pluriaggravata, e l'estorsione realizzata tramite l'utilizzo dei *ransomware*; queste altro non sono che l'evoluzione delle pratiche fraudolente ed estorsive tradizionali.

Particolare interesse suscita la frode informatica, la cui introduzione, avvenuta già con la L. 23 dicembre 1993, n. 547, si è imposta a causa delle difficoltà di applicare lo schema tradizionale della truffa alle ipotesi in cui ad essere investito dalla condotta decettiva non fosse una persona, ma il sistema informatico di pertinenza quest'ultima.

Ancora una volta, ampio spazio viene dedicato al problema del rapporto tra reati, segnatamente nelle ipotesi di frode informatica, che costituisce spesso la punta dell'*iceberg* di una progressione criminosa a cui appartengono anche i reati puniti agli artt. 615-*ter* e *quater* c.p. Parimenti problematico risulta il rapporto tra l'art. 493-*ter* c.p. e la fattispecie aggravata della frode informatica di cui ai commi 2 e 3 dell'art. 640-*ter* c.p., specie nei frequenti casi di clonazione della carta di credito.

In tali ipotesi, il criterio di specialità e l'istituto del reato complesso, riconosciuto anche di recente dalle Sezioni unite della Suprema Corte nei casi di

progressione criminosa integranti un'ipotesi di frode informatiche pluriaggravata, costituiscono due strumenti imprescindibili e generalmente idonei a comporre i suddetti conflitti interpretativi. Tuttavia, l'introduzione di nuove fattispecie di reato, anche per fatti che già entravano nell'ombrello applicativo delle norme previgenti, ha reso necessario l'affiancamento di criteri ulteriori rispetto a quello *ex* art. 15 c.p., pena l'avallo di esiti contrastanti con il principio di proporzionalità del trattamento sanzionatorio.

Infine, a completamento del particolareggiato quadro dei *cybercrimes*, l'Opera affronta i reati di reimpiego dei capitali di provenienza illecita. Contrariamente a quanto detto relativamente alle precedenti categorie, l'Autrice rileva l'efficacia dello stesso sistema repressivo, approntato dal legislatore ben prima della spinta sovranazionale, in quanto idoneo ad applicarsi alle diverse varianti del riciclaggio – quale, in particolare, il *cyberlaundering*.

Al fine di corroborare ulteriormente quanto già argomentato e di fornire uno strumento di confronto, l'Autrice dedica un ampio capitolo allo studio degli ordinamenti tedesco e spagnolo e, in particolare, all'evoluzione diacronica delle relative discipline in materia. Il metodo adottato è analitico e fondato su di un costante confronto tra le diverse scelte di politica criminale, pur senza dimenticare le differenze strutturali tra i diversi sistemi oggetto di ricerca. Nondimeno, l'analisi non risulta una mera ricognizione delle analogie e delle differenze esistenti tra i diversi Stati europei considerati, priva quindi di una finalità strumentale, ma, all'opposto, costituisce un'efficace occasione per verificare se l'auspicata armonizzazione in ambito europeo sia stata o meno raggiunta. Prima di concludere in senso negativo, la trattazione procede ad un'analisi delle discrasie presenti tra gli assetti normativi degli stessi Paesi, le quali, prima ancora che la disciplina, investono il metodo adottato dai diversi legislatori nazionali in sede di recepimento delle norme comunitarie.

Si segnala in merito che, se da una parte i legislatori italiano e spagnolo si sono limitati ad una pedissequa trasposizione del contenuto delle direttive, dall'altra,

lo *Strafgesetzbuch* tedesco ha subito degli interventi limitati, che meglio si conciliano al quadro normativo previgente.
A tale asimmetria nel metodo utilizzato in sede di attuazione della legislazione eurounitaria è conseguito un divario nella struttura delle fattispecie codificate.
Si consideri in via esemplificativa come viene differentemente punito il reato di frode informatica: il *Computerbetrug* tedesco (§ 263a *StGB*) è punito solo a titolo di dolo specifico, differentemente dalla frode informatica di cui all'art. 640-*ter* c.p., punita a titolo di dolo generico. L'*estafa informática* (art. 249.1 lett. a) *Código penal*), punendo la manipolazione informatica o ogni "altro simile artifizio", in presenza del trasferimento di un "valore patrimoniale attivo", si distingue per l'ampiezza dell'ambito applicativo.
A conclusioni non del tutto dissimili è possibile approdare in relazione alle diverse formulazioni del reato di indebito utilizzo degli strumenti di pagamento diversi dal contante.
Ma non terminano qui le problematiche originate dal disarmonico recepimento della disciplina eurounitaria; invero, talune questioni interpretative e definitorie non affrontate, o affrontate solo superficialmente, dal legislatore europeo si sono trascinate sino a gravare sul diritto positivo dei singoli Stati. In primo luogo, l'Autrice segnala come l'eterogeneità della disciplina degli preparatori sia imputabile all'assenza di una chiarezza alla fonte, ossia nelle norme europee istitutive degli obblighi di incriminazione di tali fatti. Peraltro, il legislatore comunitario non si preoccupa di distinguere questi ultimi dalle condotte che, pur essendo prodromiche alla commissione di altri delitti, manifestano un disvalore autonomo e, pertanto, contestabile isolatamente.
Il diritto sovranazionale pecca di chiarezza anche quanto alla diversificazione tra la fattispecie di frode informatica e quelle collaterali di indebito utilizzo e falsificazione dei metodi di pagamenti diversi dal contante; anche in questo caso, come la trattazione dà ampiamente conto, il problema viene trasposto nella legislazione degli Stati membri.

Per di più, se si considera che, come viene spesso sottolineato nella trattazione, gli ordinamenti nazionali erano già in buona parte conformi alle sopravvenute norme sovranazionali, non si può che accogliere la seguente conclusione: l'impulso armonizzatore del diritto eurounitario, in una sorte di eterogenesi dei fini, ha prodotto maggiori distanze tra gli ordinamenti nazionali rispetto a quelle preesistenti.

Il problema, peraltro, non è affatto irrilevante se si considera che molti dei fenomeni criminali commessi nel cyberspazio operano in una dimensione transazionale; per tale motivo, si rende quanto più necessario uno sforzo di armonizzazione condiviso tra le diverse comunità statuali interessate.

La riferita insoddisfazione per il *modus operandi* seguito dal legislatore europeo e per le censurabili soluzioni adottate dai diversi Stati è la premessa che conduce l'Autrice ad elaborare la *pars construens* dell'Opera. Vengono così raggiunte conclusioni di respiro generale, seguite da soluzioni operative vagliate con precisione tecnica.

Ribadito che il mondo digitale non può costituire una zona franca sottratta all'applicazione del diritto penale, l'analisi si concentra sull'individuazione del metodo maggiormente idoneo a garantire una efficace repressione degli illeciti commessi nel *web* nel contesto nazionale, internazionale ed europeo.

In primo luogo, preliminari sono le considerazioni sulla collocazione sistematica dei reati cibernetici e informatici: pur dovendosi condividere il giudizio positivo circa la rinuncia del legislatore di introdurre un Titolo *ad hoc*, la ripartizione interna dei suddetti reati andrebbe meglio congeniata. Invero, rilevata la crisi della tradizione bipartizione tra reati commessi con cooperazione della vittima e quelli, all'opposto, caratterizzati da unilateralità dell'offesa, non può che essere abbandonata la dicotomia accolta dal nostro Codice, che rappresenta proprio la proiezione della suddetta bipartizione, tra fattispecie commesse "mediante violenza" e "mediante frode". Pertanto, per nulla peregrina appare la proposta di istituire una nuova sottocategorizzazione basata

sull'uniformità della condotta punita dai reati cibernetici e informatici, che verrebbero così inseriti in microgruppi, come le "frodi", i "danneggiamenti" e così via.
Inoltre, al fine di incrementare l'efficacia della repressione dei reati *online* andrebbero introdotti dei criteri realisticamente idonei a determinare la giurisdizione e la competenza territoriale; tra questi, quello della personalità passiva, il quale permetterebbe di disancorare l'individuazione del giudice munito di giurisdizione e competenza territoriale dal *locus commissi delicti*, la cui identificazione risulta assai ardua, tenuto conto della dimensione virtuale delle condotte analizzate.
Un'ulteriore condivisibile proposta riguarda l'ambito della cooperazione tra pubblico e privato, strumento che, specialmente a fronte del tardivo e inefficace inserimento dei reati cibernetici nel d.lgs. 231/2001, andrebbe implementata anche attraverso l'inserimento di obblighi di segnalazione degli illeciti da parte degli enti.
Inoltre, come si ha già avuto modo di sottolineare a più riprese, si rende necessario un intervento riformatore in tema di concorso di reati. Per far fronte alla successione di norme incriminatrici ridonanti e tra loro sovrapponibili, che spesso differiscono per la sola finalità soggettiva programma criminoso, l'Autrice propone un riordino della materia articolato lungo diverse direttrici: in primo luogo, attraverso l'abrogazione delle fattispecie superflue, che, sovrapponendosi ad altre previgenti, hanno creato una duplicazione della tutela. In secondo luogo, un esito parimenti utile può essere raggiunto tramite l'introduzione di clausole di sussidiarietà nelle fattispecie che puniscono gli atti preparatori.
In aggiunta, per quanto attiene ai rapporti tra i reati patrimoniali, un'efficace soluzione coinciderebbe con la ridefinizione delle circostanze aggravanti e la conseguente configurazione di reati complessi, al quale eviterebbe a monte il problema della qualificazione del concorso tra fattispecie criminose.

Infine, le soluzioni più ambiziose aspirano ad una revisione della disciplina di parte generale del concorso di reati, in funzione di una sua razionalizzazione e maggiore coerenza sistematica.

In particolare, pur riconoscendone l'ardua percorribilità, viene prospettata la positivizzazione di ulteriori criteri – *in primis*, quello di consunzione-assorbimento -, che, sulla scorta di quanto previsto dall'art. 8 del Codice penale spagnolo, si affiancherebbero così al principio di specialità. Tuttavia, nemmeno tale opzione di politica normativa dipanerebbe i dubbi interpretativi; anzi, la somma di criteri che conducono astrattamente ad esiti tra loro diversi non farebbe altro che produrre maggiori incertezze applicative. Per una soluzione alternativa, torna utile in questa sede lo spunto offerto dal modello tedesco in materia di *Tateinheit* (§52 *StGB*): l'esclusiva applicazione della pena prevista per il reato più grave potrebbe trovare applicazione per espressa previsione legislativa nelle ipotesi di fattispecie poste in rapporto di progressione criminosa. Tale intervento potrebbe essere operato tramite la riforma del paradigma normativo dell'art. 81 c.p. che regola il reato continuato, ovvero tramite l'introduzione di una disciplina derogatoria a quest'ultimo, applicabile ai soli reati cibernetici e informatici, sulla scorta di quanto già previsto all'art. 326 del codice della crisi d'impresa per i casi di pluralità di fatti di bancarotta.

Imprescindibile è il ruolo del diritto unionale, il quale dovrebbe astenersi dall'imporre agli Stati lunghe elencazioni di fatti da punire, preferendo piuttosto un approccio coerente con i principi di sussidiarietà e di frammentarietà del diritto penale. In altre parole, dalle norme sovranazionali andrebbero rimosse le fattispecie superflue e di per sé inoffensive, che reprimono condotte neutre da un punto di vista oggettivo.

Inoltre, lo stesso legislatore europeo dovrebbe tenere distinti gli atti preparatori dalle condotte che, ancorché prodromiche alla commissione di ulteriori reati offensivi del patrimonio, costituiscono "ipotesi tipizzate di concorso di persone nel reato". In merito a ciò, si pensi al traffico di dati personali e identificativi

nell'ambito del fenomeno del *Cybercrime-as-a-service*: le condotte che ne compongono lo schema, a parere dell'Autrice, non dovrebbero essere punite con una pena ridotta, ma, all'opposto, alle stesse andrebbe ancorato un sistema sanzionatorio proporzionato al disvalore sociale e alla concreta pericolosità di cui si fanno portatrici.

Alla luce delle riflessioni svolte e delle soluzioni prospettate, l'opera monografica di Chiara Crescioli si distingue per l'ampiezza del campo di indagine, l'attualità della materia trattata e per l'approccio pragmatico, mai avulso dalle problematiche concretamente riscontrabili nella prospettiva applicativa del diritto penale. In definitiva, l'apporto interpretativo costituisce una valida guida per l'operatore del diritto penale nella soluzione delle questioni ermeneutiche sollevate dalla costante evoluzione tecnologica.