SISTEMA PENALE

FASCICOLO

4/2021

ISSN 2704-8098

Sistema penale (*SP*) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.
La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale.
Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.
La *Rivista* si uniforma agli standard internazionali definiti dal *Committe on Publication Ethics* (COPE) e fa proprie le relative linee guida.

Peer review I contributi che la direzione ritiene di destinare alla sezione "*Articoli*" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezione "*Altri contributi*" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.
Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione Per la citazione dei contributi presenti nei fascicoli di *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen.* (o *SP*), 1/2020, p. 5 ss.

SISTEMA PENALE

4/2021

LE FATTISPECIE DI DANNEGGIAMENTO INFORMATICO: UNA COMPARAZIONE TRA ITALIA E CINA

di Emanuele Riva

L'elaborato sviluppa la comparazione tra Italia e Cina nel campo dei delitti di danneggiamento informatico. È approfondita, in primo luogo, la cornice costituzionale dei due Paesi e la diversa valenza del principio di legalità, che si riflette, in definitiva, sulle caratteristiche della fattispecie incriminatrice. Vengono, quindi, analizzate le singole fattispecie evidenziando gli elementi e le scelte punitive comuni ai due ordinamenti: lo studio è condotto sul piano del bene giuridico tutelato, del fatto tipico e del rapporto tra danneggiamento informatico e invio di virus informatici. Si cerca, infine, di comprendere le ragioni dell'inattesa affinità tra i due sistemi.

SOMMARIO: 1. Introduzione. – 2. Il quadro sanzionatorio nell'ordinamento italiano. – 3. La legislazione cinese: l'art. 286 del codice penale. – 4. Danneggiamento di sistemi e danneggiamento di dati. – 5. L'oggetto di tutela: funzione e funzionamento del sistema informatico. – 6. Il rapporto tra invio di virus e danneggiamento informatico. – 7. Conclusioni.

1. Introduzione.

Diversi scritti di diritto penale dell'informatica si aprono con una riflessione circa il ruolo e la diffusione delle "nuove tecnologie", quasi a doversi giustificare di aver intrapreso una materia tanto tecnica e settoriale. A ben vedere, le tecnologie informatiche sono al giorno d'oggi la normalità, un elemento imprescindibile del vivere quotidiano[1]. Così, il diritto dell'informatica non può più ritenersi un'avanguardia insolita per pochi giuristi appassionati: il diritto dell'informatica è *il* diritto dei nostri giorni.

Si tratta, infatti, di un argomento vivo e attuale, che impone una riflessione sempre più attenta agli sviluppi tecnologici e al progressivo schiudersi di nuove sfide per il giurista[2]. Il diritto penale dell'informatica è parte del c.d. diritto dell'era digitale: è, quindi, un diritto essenzialmente transnazionale[3]. Detti aspetti ben si colgono nella

[1] L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi, S. Canestrari, A. Manna, *Cybercrime*, 2019, Milano, 37-38.

[2] Per alcuni approfondimenti sulle nuove frontiere del diritto italiano dell'informatica: C. BENETAZZO, *ICT e nuove forme di interazione tra cittadino e Pubblica Amministrazione*, in *MediaLaws*, n. 2, 2020, 263-265; P. INSOLERA – S. ROMANO, *Processo penale "a distanza" e diritto alla privacy: possibili profili di contrasto*, in *MediaLaws*, n. 2, 2020.

[3] G. PASCUZZI, *Il diritto dell'era digitale*, Bologna, 2016, 333.

comparazione con la disciplina cinese. In particolare, si è scelto di approfondire i delitti di danneggiamento informatico, sia perché sanzionano fenomeni largamente diffusi e in aumento[4], sia perché si tratta delle norme che meglio si prestano ad evidenziare le caratteristiche costituzionali e le scelte punitive dei due ordinamenti.

La Cina rappresenta, oggi, uno dei modelli più evoluti di integrazione della dimensione digitale nelle dinamiche quotidiane del tessuto sociale ed economico[5]: basti pensare alla diffusione delle c.d. *superApp*[6] o al costante processo di ricerca e sviluppo di nuove tecnologie, condotto, da ultimo, nel campo dell'intelligenza artificiale[7]. Le stesse Istituzioni della *PRC* rivolgono grande attenzione ai temi della modernizzazione[8] e della digitalizzazione[9], tanto che il progresso tecnologico può riconoscersi come un elemento essenziale della Costituzione formale[10] e sostanziale del Paese.

La Cina è altresì Patria di un diritto diverso dal nostro. Sono diversi i presupposti storico-culturali: tradizione, società e cultura giuridica[11]. Sono diverse le scelte politiche più recenti: l'ispirazione costituzionale, di matrice leninista-maoista, si ripercuote, come si vedrà, sulle caratteristiche essenziali del diritto penale. A ciò si aggiunga che la Repubblica Popolare non ha aderito alla Convenzione di Budapest[12] sul crimine informatico.

Date queste premesse, ci si potrebbe aspettare che la comparazione tra i due Paesi si riduca ad una mera rassegna di differenze. Ma non è così.

---

[4] Si considerino il più recente rapporto Clusit – associazione italiana per la sicurezza informatica e il rapporto Allianz Global Corporate & Specialty (AGCS) dell'ottobre 2020.

[5] S. PIERANNI, *Red Mirror. Il nostro futuro si scrive in Cina*, Bari-Roma, 2020, *passim.*

[6] Un esempio è costituito dall'*App WeChat* con cui è possibile, ad esempio, conversare in lingue diverse avvalendosi di un sistema di traduzione istantanea, effettuare pagamenti e piccole transazioni tra utenti, prenotare una visita medica, acquistare e programmare un viaggio sui mezzi di trasporto, pagare alcuni servizi pubblici, come le bollette dell'elettricità (per l'elenco esaustivo delle funzioni di *WeChat*, si può consultare la relativa sezione dello *Store GooglePlay*, all'URL www.play.google.com). L'argomento è approfondito in S. PIERANNI, *Red Mirror*, cit., 1 ss.

[7] M. SORRENTINO, *Intelligenza artificiale: lezioni dalla Cina*, in C. Bulfoni, E. Lupano, B. Mottura (a cura di), *Sguardi sull'Asia e altri scritti in onore di Alessandra Cristina Lavagnino*, Milano, 2017,113-115. Sul rapporto tra intelligenza artificiale, società e legislazione in Cina: L. WEIQIU, *"Technology-Society+Economy" Paradigm of AI Legislation*, in *Wǔhàn dàxué xuébào* (武汉大学学报), n. 1, 2020, 65.

[8] Per un utile approfondimento: Q. YUJUN, *Modernization and Legislation of Scientific and Technical Administration*, in *Kējì yǔ fǎlǜ* (科技与法律), n. 4, 1995.

[9] In Cina sono state istituite, ad esempio, sia la *Cyberspace Administration of China* (*Guójiā hùliánwǎng xìnxī bàngōngshì* - 国家互联网信息办公室; letteralmente: Ufficio nazionale d'informazione su *Internet*), sia la *Central Cyberspace Affairs Commission* (*Zhōngyāng Wǎngluò Ānquán Hé Xìnxī Huà Wěiyuánhuì* - 中央网络安全和信息化委员会).

[10] Come si evince dal Preambolo e dagli artt. 14 e 47 della Costituzione della Repubblica Popolare Cinese.

[11] Il tema è sviluppato in J. ZHANG, *The Tradition and Modern Transition of Chinese Law*, Springer, 2008; I. CARDILLO, Y. RONGGEN, *La cultura giuridica cinese tra tradizione e modernità*, in Quaderni fiorentini XLIX (2020), pp. 97-134 (contributo pubblicato sul sito dirittocinese.com, all'URL https://dirittocinese.com/2020/10/22/la-cultura-giuridica-cinese-tra-tradizione-e-modernita/).

[12] Ci si riferisce alla *Convention on Cybercrime*, stipulata a Budapest, il 23 novembre del 2001.

Nel *Codice penale della Repubblica popolare cinese*[13] (in seguito, anche solo codice penale o codice penale cinese) si prevedono fattispecie dedicate al danneggiamento informatico (precisamente, l'art. 286), che corrispondono, in certo modo, ai quattro articoli (artt. 635-*bis*; 635-*ter*; 635-*quater*; 635-*quinquies*) introdotti nel codice penale italiano. La presente ricerca si occupa di approfondire ciò che accomuna i due ordinamenti e di individuare le ragioni di tale convergenza.

2. Il quadro sanzionatorio nell'ordinamento italiano.

Sotto la spinta del Consiglio d'Europa[14], il Legislatore italiano, con la L. 547/1993, ha introdotto nel codice penale l'art. 635-*bis*, rubricato «Danneggiamento di sistemi informatici e telematici»[15]. Ratificata la Convenzione di Budapest, la norma è stata sostituita, ai sensi dell'art. 5 della L. 48/2008, dalle quattro fattispecie che compongono l'apparato sanzionatorio ora vigente.

L'art. 635-*bis*, nella nuova versione, punisce le condotte di danneggiamento o soppressione di "*informazioni, dati o programmi informatici altrui*"[16]. Le medesime condotte sono contemplate dall'art. 635-*quater*: tale norma, tuttavia, si caratterizza per il diverso diverso oggetto materiale dell'evento, costituito dai «sistemi informatici e telematici».

Tale impostazione "binaria" viene ripresa anche dagli artt. 635-*ter* e 635-*quinquies* che, tuttavia, si riferiscono ai dati e ai sistemi informatici "*utilizzati dallo Stato o da altro*

---

[13] In lingua originale: *Zhōnghuá rénmín gònghéguó xíngfǎ* (中华人民共和国刑法). Il testo è stato promulgato il 1° luglio del 1979 ed è stato profondamente riformato nel 1997, entrando, così, in vigore nell'ottobre dello stesso anno. Si noti che la legge penale del 1979 ammetteva il ricorso all'analogia (art. 79), benché fosse prevista la supervisione da parte della Corte Suprema del Popolo: solo diciotto anni più tardi è stato sancito il divieto di ricorrere al procedimento analogico. Come nota il Picotti, tale divieto non è, tuttavia, contemplato nella Costituzione, ma si deduce dall'affermazione del principio di legalità, in base all'art. 3 dello stesso codice penale cinese: L. PICOTTI, *Offensività ed elemento soggettivo del reato nel codice penale della repubblica popolare cinese*, in *Diritto Penale XXI Secolo*, n. 1, 2010, p. 54. Sull'evoluzione del diritto penale in Cina: I. CARDILLO, *Lo sviluppo del diritto penale cinese dalla fondazione della repubblica popolare ad oggi*, in *Diritto Penale XXI Secolo*, n. 2, 2018, 261-274.
Per la traduzione italiana del codice penale cinese si fa riferimento all'autorevole contributo del Prof. Shenkuo Wu, in S. WU (traduzione di), S. VINCIGUERRA (revisore della traduzione e curatore dell'edizione), *Il codice penale della repubblica popolare cinese*, in *Diritto Penale XXI Secolo*, Anno IX, 2010.

[14] Il riferimento è alla Raccomandazione No. R. (89)9 del Consiglio d'Europa (Comitato dei Ministri), adottata il 18 gennaio 1989.

[15] Il testo introdotto dall'art. 9 della l. 547/1993 prevedeva che «chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni. Se ricorre una o più delle circostanze di cui all'articolo 635 c. 2, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni».

[16] Il secondo comma individua una circostanza aggravante se il fatto è commesso con violenza alla persona o con minaccia ovvero «con abuso della qualità di operatore del sistema». Va rilevato, a tal proposito, che la figura dell'operatore di sistema si riconosce in colui che, per le funzioni svolte, si trova nella posizione di intervenire continuativamente sul sistema informatico. Tale aggravante ricorre nei principali reati informatici previsti dal codice e persegue, in definitiva, la violazione del rapporto di fiducia che intercorre tra titolare del sistema e *system operator*.

ente pubblico o comunque di pubblica utilità". Tali ultime norme, invero, si distinguono anche sotto il profilo della struttura del reato. Nell'ipotesi in cui l'oggetto materiale della condotta sia "di pubblica utilità", il Legislatore ha, infatti, previsto una significativa anticipazione della soglia di rilevanza penale. Sanzionando "i fatti diretti a" danneggiare i dati o i sistemi "pubblici", gli artt. 635-*ter* e 635-*quinquies* configurano, in realtà, un reato di pericolo[17]: il delitto si consuma a prescindere dall'effettivo verificarsi dell'evento di danneggiamento.

L'anticipazione della rilevanza penale dipende, così, dalla qualificazione dell'oggetto materiale della condotta: una scelta legislativa che, tuttavia, connota il reato di una certa indeterminatezza.

Le norme richiamate si riferiscono, in primo luogo, ai dati e ai sistemi informatici "utilizzati da un ente pubblico o dallo Stato": si tratta di un'espressione vaga, foriera di dubbi interpretativi e applicativi. Non è chiaro, ad esempio, se ricorra il requisito in esame solo nel caso in cui i dati o i sistemi informatici facciano parte della dotazione stabile dell'ente pubblico oppure anche qualora l'ente venga ad utilizzare tali strumenti solo occasionalmente.

Risulta, in secondo luogo, ancora più problematico stabilire quando ricorra la "pubblica utilità" dell'oggetto materiale. Per fare chiarezza sulla portata di tale espressione, vi è chi ha proposto di considerare soddisfatto il requisito in esame qualora i dati o il sistema siano «comunque di interesse pubblico»[18], rilevando, in questo senso, «l'utilità sociale dell'oggetto dell'aggressione»[19] e le conseguenze lesive per la tutela degli interessi pubblici. Tale soluzione interpretativa non pare, tuttavia, risolvere il *vulnus* di determinatezza che affligge le fattispecie in esame. Non sempre sarà possibile conoscere e riconoscere, *ex ante*, l'utilità sociale di un dato informatico o di un sistema informatico: sicché, in definitiva, la portata di queste espressioni e, di conseguenza, l'estensione della rilevanza penale, si conosceranno, nell'ipotesi concreta, solo al termine del giudizio.

3. La legislazione cinese: l'art. 286 del codice penale.

L'art. 286 del codice penale cinese contempla il reato di danneggiamento informatico. In particolare, nella traduzione italiana[20], il primo comma recita come segue: *chiunque, in violazione delle disposizioni statali, compiendo operazioni di cancellazione, modificazione, aggiunzione, impedimento al funzionamento di un sistema informatico o*

---

[17] I. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Riv. it. Dir. proc. pen.*, 2012, 204 ss.; C. PARODI e V. SELLAROLI (a cura di), *Diritto penale dell'informatica. I reati della rete e sulla rete*, 2020, 595; D. PAOLANTI, *Il danneggiamento di sistemi informatici o telematici di pubblica utilità*, in *studiocataldi.it*.

[18] V. DESTITO, *Digesto delle discipline penalistiche*, Torino, 2010 (aggiornamento), 751.

[19] *Ibid*.

[20] La traduzione è sempre tratta da S. WU, *Il codice penale della Repubblica Popolare cinese*, cit. Una traduzione ufficiale in lingua inglese della legge penale cinese è consultabile a questa pagina sul sito ufficiale della Missione permanente della Repubblica Popolare Cinese presso le Nazioni Unite.

telematico, cagiona il malfunzionamento del sistema suddetto, qualora vi sia una conseguenza grave, è punito con la reclusione pari o inferiore a cinque anni o con l'arresto.

L'articolo prosegue con un secondo comma, con il quale viene sanzionato *chiunque, in violazione delle disposizioni statali, compie operazioni di cancellazione, modificazione, aggiunzione ai dati o programmi applicativi che sono conservati, trattati o trasmessi in un sistema informatico o telematico*.

Un terzo comma della medesima norma sanziona il danneggiamento informatico perpetrato mediante l'uso di programmi dannosi: ci occuperemo di tale ipotesi affrontando il tema dei virus informatici.

La lettura dell'art. 286 del codice penale può destare, a prima vista, perplessità. Può sorprendere, infatti, che la norma cinese ricorra ad espressioni particolarmente vaghe: il fatto tipico è punibile, ad esempio, solo «qualora vi sia una conseguenza grave»[21]. Similmente, la pena è aumentata qualora le conseguenze siano «particolarmente gravi»[22]. Come è evidente, si tratta di uno stile legislativo assai distante dal modello di sufficiente determinatezza perseguito dal legislatore penale occidentale[23].

Una simile tecnica di *drafting* è, però, coerente con i princìpi costituzionali accolti dall'ordinamento cinese. Si tratta di un aspetto che merita di essere approfondito.

Partiamo dal presupposto che il principio di sufficiente determinatezza della fattispecie penale rappresenta un'estrinsecazione necessaria del principio di legalità. È pacifico, infatti, che quando la formulazione legislativa lascia margini eccessivi alla valutazione discrezionale dell'interprete, il principio legalitario viene, di fatto, svuotato del proprio significato e della propria funzione. È il tema, se vogliamo, delle c.d. norme penali in bianco. È altrettanto riconosciuto che il principio di legalità costituisce, a sua volta, un ineludibile «corollario del principio della divisione dei poteri»[24]. Da queste brevi premesse possiamo dedurre l'esistenza di un'interconnessione logica tra principio di separazione dei poteri, principio di legalità e principio di sufficiente determinatezza della legge penale, tale che ove non sia riconosciuto il primo, sfumino di conseguenza anche le altre garanzie considerate: è questo il caso del sistema cinese.

La Costituzione della Repubblica Popolare Cinese non riconosce il principio di divisione dei poteri: almeno formalmente, non è nemmeno corretto parlare di "poteri", al plurale. L'art. 2 della Costituzione cinese, infatti, afferma solennemente che «*All power in the People's Republic of China belongs to the people*»[25]. Tale impostazione è espressione del modello di centralismo democratico di matrice leninista, vero e proprio principio-

---

[21] Il testo in lingua originale dell'art. 286 parla di *Hòuguǒ yánzhòng de* (**后果**严重的), letteralmente "conseguenze serie".

[22] In questo caso, la pena prevista è superiore ai cinque anni di reclusione: *Hòuguǒ tèbié yánzhòng de, chǔ wǔ nián yǐshàng yǒu qí túxíng* (**后果特**别严重的，处五年以上有期徒刑).

[23] F. PALAZZO, *Legalità e determinatezza della legge penale: significato linguistico, interpretazione e conoscibilità della regola iuris*, in G. Vassalli (a cura di), *Diritto penale e giurisprudenza costituzionale*, Napoli, 2006, 49 ss.

[24] G. FIANDACA – E. MUSCO, *Diritto Penale. Parte Generale*, Bologna, 2014 (VII edizione), 48. Sul punto anche M. SINISCALCO, *Giustizia penale e Costituzione*, Milano, 1968, 40-41.

[25] La traduzione ufficiale in lingua inglese è tratta dal sito del Consiglio di Stato della Repubblica Popolare Cinese (*www.gov.cn*); in lingua originale: *Zhōnghuá rénmín gònghéguó de yīqiè quánlì shǔyú rénmín* (**中**华人民共和国的一切权力属于人民).

cardine del sistema costituzionale cinese[26]. Il tema meriterebbe, invero, una trattazione a sé. In questa sede, interessa focalizzarsi soltanto sul rifiuto del principio di divisione dei poteri: basti considerare, del resto, che soltanto entro un quadro costituzionale che sancisca tale rifiuto, il Partito Comunista può esplicare la propria attività di supervisione e direttiva[27] nei confronti delle diverse articolazioni dell'apparato amministrativo e istituzionale, ivi compresi gli organi legislativi e giudiziari[28].

Il rifiuto formale della divisione dei poteri determina una concezione "debole" del principio di legalità. È stato osservato, a tal proposito, che nell'ordinamento cinese «basta una riserva relativa, che lasci ampi varchi agli apporti di fonte amministrativa e di fonte giudiziaria, in cui la direttiva politica del partito unico [possa] spiegarsi agevolmente»[29]. In questo senso si deve leggere la clausola d'illiceità speciale contemplata dall'art. 286, con la quale si subordina la configurabilità del reato di danneggiamento informatico alla violazione delle «disposizioni statali»[30]. Si tratta, invero, di una clausola piuttosto frequente nelle disposizioni del codice penale cinese[31]. Orbene, in base all'art. 96 del codice penale, con l'espressione «disposizioni statali» devono intendersi non soltanto le leggi emanate dall'Assemblea Nazionale del Popolo (o dal Comitato Permanente) ma anche le misure di carattere amministrativo e le decisioni adottate dal Consiglio di Stato[32].

Ora, è chiaro che simili rinvii a fonti non legislative finiscono per atrofizzare il principio di legalità. Di conseguenza, in un ordinamento in cui la divisione dei poteri e il principio legalitario non sono garanzie riconosciute e ineludibili, non ci si può aspettare che la norma penale abbia un alto grado di determinatezza. Del resto, la tecnica di *drafting* perseguita dal Legislatore cinese è proprio quella di lasciare il maggiore spazio all'interprete.

Si spiega così l'utilizzo di espressioni generiche nel testo dell'art. 286 della legge penale cinese. Non si tratta di un *deficit* nella tecnica redazionale adottata dal Legislatore, bensì, all'opposto, di una scelta consapevole e coerente con i valori costituzionali della Repubblica Popolare.

---

[26] W. CHUANZHI, *Democratic Centralism: The Core Mechanism in China's Political System*, in *Qiushi Journal*, n. 4, 2013; G. CRESPI REGHIZZI, *Centralismo democratico* (voce), in *Digesto delle discipline privatistiche*, Torino, 1988, 268; C. MUGELLI, *Indipendenza e professionalità del giudice in Cina* (tesi di dottorato), Firenze, 2012, 23-25.

[27] S. VINCIGUERRA, *Impressioni di un penalista italiano alla lettura del codice penale cinese*, in *Diritto Penale XXI Secolo*, n. 1, 2010, 39.

[28] Benché, infatti, l'art. 126 della Costituzione cinese sancisca che i Tribunali del Popolo esercitano il potere giudiziario in modo indipendente, l'art. 128 precisa, tuttavia, che la Corte Suprema del Popolo è responsabile nei confronti dell'Assemblea Nazionale del Popolo e del suo Comitato Permanente. Inoltre, l'art. 67 prevede che il Comitato Permanente ha il potere di supervisionare i lavori della Corte Suprema del Popolo, ovvero di nominarne o rimuoverne, su raccomandazione del presidente della stessa Corte, i vicepresidenti e i giudici, i membri del suo comitato giudiziario e il presidente della corte militare.

[29] S. VINCIGUERRA, *Impressioni di un penalista italiano,* cit., 39.

[30] La norma si riferisce, letteralmente, alla "violazione delle norme nazionali": *Wéifǎn guójiā guīdìng* (违反国家规定).

[31] Si vedano, a titolo di esempio, gli artt. 137; 184; 222; 225; 285; 288 del codice penale cinese.

[32] Il Consiglio di Stato (*Guówùyuàn*; 国务院) non è, in Cina, un organo di giustizia amministrativa, ma è il massimo organo di governo della Repubblica Popolare.

Si può aggiungere, infine, una considerazione. La dottrina giuridica cinese ha valorizzato l'impiego di espressioni generiche con specifico riferimento alle norme incriminatrici in materia informatica[33]. Shan Yuming, in particolare sostiene che proprio le clausole più generiche (come le «circostanze gravi» previste dall'art. 286)[34] possono essere sfruttate in sede interpretativa, sia per limitare l'applicabilità della fattispecie penale, in ossequio al principio di *extrema ratio*, sia per adeguare e aggiornare, in concreto, il carico sanzionatorio delle diverse fattispecie informatiche[35]. La norma penale che consenta la massima discrezionalità interpretativa sarebbe, dunque, la più idonea a perseguire un fenomeno dinamico e mutevole come quello informatico.

Fornite, così, le coordinate essenziali per comprendere la fattispecie dell'art. 286, si può procedere con alcune considerazioni in prospettiva comparata.

4. Danneggiamento di sistemi e danneggiamento di dati.

Sia in Cina sia in Italia si prevedono norme differenti a seconda che si tratti di danneggiamento di dati oppure di danneggiamento di sistemi informatici. All'art. 635-*bis* del codice penale italiano corrisponde, per certi versi, il secondo comma dell'art. 286 del codice penale cinese[36], così come all'art. 635-*quater* corrisponderebbe l'art. 286, primo comma[37].

Non si tratta di un'impostazione scontata. Basti solo ricordare che il reato di danneggiamento informatico introdotto in Italia con la L. 547/1993 contemplava, sotto un'unica fattispecie, sia il danneggiamento dei dati sia il danneggiamento dei sistemi[38].

Viene, dunque, da chiedersi quale sia la *ratio* alla base di una simile scelta legislativa. A ben vedere, le motivazioni di tale regime non sono le stesse nei due ordinamenti.

Con riguardo al sistema penale italiano, un dato risulta evidente. La forbice edittale prevista per l'aggressione ai sistemi varia da «uno a cinque anni di reclusione»; nel caso di attacco ai dati e programmi, si prevede, invece, la reclusione «da sei mesi a tre anni». Il Legislatore del 2008 ha, quindi, riconosciuto una maggiore carica lesiva nel

---

[33] S. YUMING, *The Current Situation of Network Crime Legislation and its Direction in China*, in *Héběi fǎxué* (**河北法学**), n. 6, 2018.

[34] *Ibid.*; con le parole dell'Autore: *Wèi shìyìng wǒguó fànzuì gàiniàn cǎiqǔ dìngxìng qiě dìngliàng de lìfǎ jiédìng móshì yǔ wǎngluò fànzuì jìliàng duìxiàng hǎiliàng huà de xiànshí xūyào* (为适应我国犯罪概念采取定性且定量的立法界定模式与网络犯罪计量对象海量化的现实需要).

[35] In lingua originale, si legge: *Děng dìngliàng yāoqiú zuòwéi fǎdìng xíng shēnggé de tiáojiàn* (**等定量要求作**为法定刑升格的条件).

[36] X. LI, *Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime*, in *International Journal of Cyber Criminology*, n. 2, 2015, 195.

[37] X. LI, *Regulation of Cyber Space*, cit., 194. Sul punto, anche P. YONG, *Comparative research on "Convention on Cybercrime" and Chinese relevant Legislation*, in *coe.int*, 2. In particolare, l'Autore accosta i primi paragrafi dell'art. 286 del codice penale cinese all'art. 5 della Convezione di Budapest.

[38] L'art. 635-*bis* c.p. come introdotto dalla L. 547/1993 si riferiva a «chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui».

danneggiamento del sistema informatico rispetto al danneggiamento dei soli dati. Quanto detto, trova conferma analizzando anche il regime di procedibilità previsto dalle due norme: per il delitto di cui all'art. 635-*bis* si procede a querela della persona offesa; il reato di cui all'art. 635-*quater* è, invece, procedibile d'ufficio.

L'impostazione configurata dalla L. 48/2008 discende dagli artt. 4[39] e 5[40] della Convezione di Budapest. Va osservato, però, che la Convenzione non impone che il danneggiamento dei sistemi sia punito con sanzione più severa rispetto a quella prevista per l'attacco ai dati: si tratta, dunque, di una precisa scelta di politica criminale da parte del Legislatore italiano.

È opportuno operare, inoltre, una precisazione di ordine terminologico. Nella formulazione degli artt. 635-*bis* e 635-*quinquies* si fa riferimento a «dati, informazioni e programmi». È stato però osservato, correttamente, che la differenza tra i termini menzionati sarebbe «più che altro nominalistica»[41], dal momento che la nozione di "informazioni" non rappresenterebbe un concetto autonomo e facilmente distinguibile da quello di "dati" o "programmi". Sostanzialmente, le norme si riferiscono al danneggiamento dei dati e dei programmi, confermando, quindi, il parallelismo di fondo con l'art. 286 della legge penale cinese, ove si menzionano (opportunamente) soltanto dati o programmi[42].

Nel sistema cinese, tuttavia, la *ratio* alla base dello sdoppiamento delle fattispecie non si può ricostruire in termini di offensività. La pena è, infatti, la medesima, sia che si tratti di danneggiamento di sistemi, sia che si tratti di danneggiamento di dati.

Ad un'analisi attenta dell'art. 286, si osserva che le fattispecie previste dai primi due commi non sono parallele, ma, piuttosto, complementari.

È stato notato che soltanto la prima norma, quella riferita al sistema informatico, è idonea a perseguire il danneggiamento dell'«*hardware equipment*»[43]: l'aggressione fisica al bene protetto rileva tanto in quanto cagioni il malfunzionamento del *computer system.* Di converso, l'attacco ai dati e programmi informatici assume rilevanza penale esclusivamente come attività di *hacking* in senso stretto, perpetrata attraverso operazioni informatiche. La differenza tra le due fattispecie consiste, dunque, nella possibilità o meno di configurare l'ipotesi di danneggiamento "fisico". In questo senso, soltanto il *computer system*, come complesso *hardware*, è tutelato sia dal cyberattacco vero e proprio, sia dalla lesione delle componenti materiali, come, per esempio, nel caso di

---

[39] L'art. 4 della Convezione prevede che: «*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right* (…)».

[40] L'art. 5 della Convenzione prevede che: «*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data*».

[41] V. DESTITO, *Digesto*, cit., 750.

[42] Cfr. art. 286 del codice penale cinese; letteralmente, la norma si riferisce ai «dati» e alle «applicazioni»: *Shùjù hé yìngyòng chéngxù jìnxíng* (数据和应用程序进行).

[43] P. YONG, *Comparative Research*, cit., 2.

danneggiamento della scheda madre perpetrato utilizzando una bomba elettromagnetica[44].

Ma non è tutto. Bisogna osservare che la fattispecie di cui al secondo comma sanziona l'aggressione ai dati in quanto «memorizzati, elaborati o trasmessi dal sistema informatico»[45]: qualora i dati attaccati si considerino al di fuori di un sistema informatico, la condotta non sarebbe punibile[46]. Anche il danneggiamento dei dati informatici deve interferire, cioè, con il corretto funzionamento del *computer information system* menzionato nel primo paragrafo della norma.

Entrambe le norme, in definitiva, proteggono il sistema informatico, da due diverse prospettive: ecco perché si possono definire fattispecie complementari. Il primo paragrafo dell'art. 286 del codice penale sembra salvaguardare il sistema nella sua dimensione di infrastruttura *hardware*, attraverso un reato di evento che risulta integrato se la condotta del soggetto agente «cagiona il malfunzionamento del sistema»[47].

All'opposto, il secondo paragrafo dell'articolo 286 si concentra sulla sanzione delle condotte illecite propriamente informatiche, tutelando, quindi, il contenuto del sistema, i dati e i programmi. In definitiva, la sanzione del danneggiamento informatico si sviluppa, nel codice penale cinese, attraverso una duplice dimensione: quella del sistema in quanto tale, come "infrastruttura informatica", e quella del sistema come complesso di dati e programmi.

L'impostazione descritta ha delle importanti ricadute applicative. Per accertare la rilevanza penale del danneggiamento informatico serve stabilire, di volta in volta, se ricorra la nozione di *computer information system*. Come è noto, però, la definizione di sistema informatico è controversa e, talvolta, sfuggevole, tanto nel diritto cinese, quanto nel diritto italiano[48]. A tal proposito, basti considerare l'esempio del danneggiamento di

---

[44] *Ibid*. L'Autore cita espressamente l'ipotesi di «*damaging computer motherboard by using electromagnetic bomb*».

[45] S. WU, *Il codice penale della repubblica popolare cinese,* cit.

[46] P. YONG, *Comparative research*, cit., 3.

[47] L'espressione è tratta dalla preziosa traduzione in italiano del codice penale cinese: S. WU, *Il codice penale della repubblica popolare cinese*, cit.

[48] Basti una breve considerazione. Nel portale Federica dell'Università di Napoli Federico II, il "sistema informatico" è definito come infrastruttura tecnologica sulla quale poggia il sistema informativo; su brocardi.it viene invece definito come un *computer* o un insieme di più *computer* o altri apparati elettronici (es. router ecc...), tra loro interconnessi in rete: si compone sia di elementi *hardware* che *software*. La differenza tra le due nozioni è evidente, soprattutto con riferimento al requisito della "connessione alla rete"; il riferimento, inoltre, alla nozione di *computer* trasferisce il problema definitorio a quest'ultima espressione, tutt'altro che pacifica. Rientrano, con alta probabilità, nella categoria "computer", i PC, i laptop, gli smartphone, i tablet, le smart TV, i sistemi di c.d. Infotainment degli autoveicoli, gli ATM, le consolle per videogiochi e, in generale, i server, atteso che tutti i dispositivi menzionati uniscono una componente Hardware e la componente Software alla possibilità di collegarsi ad una rete. Più difficile è, invece, comprendere la distinzione tra uno smartwatch, che, alla stregua dei criteri indicati, può considerarsi un computer, e un orologio satellitare (come quelli utilizzati per monitorare l'attività sportiva): in quest'ultimo caso, il dispositivo è collegato ad una rete GPS e non è chiaro se vi sia un unico sistema informatico (orologio con satellite), se siano due sistemi distinti (orologio e satellite) oppure se non vi sia alcun sistema informatico. Similmente, ci si potrebbe chiedere se un computer non funzionante perché privo, ad esempio, della scheda madre, sia ancora considerato un sistema informatico. Il ragionamento potrebbe proseguire esplorando ulteriori ramificazioni di questo rebus linguistico pressoché inestricabile. Insomma, la realtà

un *hard disk* esterno o di una chiavetta *USB*: siamo in presenza di un *computer information system*? Se si risponde negativamente, la distruzione materiale di simili dispositivi non rientrerebbe nel fatto tipico descritto dall'art. 286 del codice penale cinese.

Se, invece, venissero hackerati i dati contenuti nell'*hard disk* o nella chiavetta, bisognerebbe comunque verificare che le informazioni danneggiate possano considerarsi «*within computer system*»[49], vale a dire conservate, trattate o trasmesse in un sistema informatico o telematico. Le considerazioni svolte rendono, ad ogni modo, evidente quanto il ruolo svolto dalla nozione di sistema informatico si riveli essenziale per configurare il reato di cui all'art. 286 del codice penale cinese. Tale problema non si pone, invece, per le norme italiane, che sanzionano anche l'aggressione di dati che non accedano ad un sistema informatico[50].

La Corte Suprema del Popolo[51] ha fornito delle indicazioni ermeneutiche per ricostruire la nozione di sistema informatico. L'argomento è affrontato nel caso-guida *No. 103: People v. Xu Qiang*[52], deciso il 9 agosto del 2016[53]. I Casi-Guida costituiscono una selezione, operata dal massimo organo giurisdizionale del Paese, di casi giudicati da corti inferiori, che vengono così dotati «*de facto* di forza vincolante»[54]. L'iniziativa, avviata nel 2010, costituisce uno strumento importante per unificare gli *standard* di interpretazione giudiziale, trattandosi di decisioni alle quali tutte le Corti, di ogni livello, possono fare riferimento: si è addirittura parlato, forse impropriamente, di "*new chinese*

---

informatica conosce svariate applicazioni ma non è chiaro quali rientrino nella definizione di "sistema informatico". Per alcune interessanti osservazioni sul linguaggio informatico, si rinvia ad A. ZOPPETTI, *Il disastro della terminologia informatica italiana di fronte all'inglese*, 14 maggio 2018.
Una definizione di sistema informatico si trova nelle fonti sovranazionali. In particolare, l'art. 1, lett. a), della Convenzione di Budapest sulla criminalità informatica definisce il sistema informatico come "*qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati*". La norma fornisce, altresì, la definizione di "dati informatici", "service provider" e "trasmissione di dati". Similmente, l'art. 2 della Direttiva 2013/40/UE fornisce una definizione di "sistema d'informazione" quale "*apparecchiatura o gruppo di apparecchiature interconnesse o collegate, uno o più dei quali svolge un trattamento automatico di dati informatici secondo un programma, nonché i dati informatici immagazzinati da tale apparecchiatura o gruppo di apparecchiature,*
trattati, estratti o trasmessi dagli stessi ai fini della loro gestione, uso, protezione e manutenzione".

[49] P. YONG, *Comparative research*, cit., 3.

[50] A. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in A. Cadoppi, S. Canestrari, A. Manna, *Cybercrime*, 2019, Milano, 779. Vi è chi ritiene, invece, debba sussistere un legame funzionale tra le «informazioni» e un sistema informatico: R. DE PONTI, *Art. 635*-bis (voce), in E. Dolcini – G. L. Gatta, *Codice Penale Commentato*, Milano, 2015, 1013.

[51] La Corte Suprema del Popolo è, in base all'art. 127 della Costituzione cinese, il massimo organo giudiziario della Repubblica popolare cinese: controlla l'amministrazione della giustizia da parte dei tribunali popolari ai vari livelli locali e dei tribunali speciali.

[52] Si tratta del caso *Zhǐdǎo ànlì 103 hào: Xúqiáng pòhuài jìsuànjī xìnxī xìtǒng àn* (指导案例103号：徐强破坏计算机信息系统案).

[53] La decisione è stata selezionata come caso-guida il 25 dicembre del 2018, dietro approvazione del *Judicial Committee* della Corte Suprema del Popolo.

[54] La definizione riportata è tratta da I. CARDILLO, *Collaborazione tra Diritto Cinese e CGCP Stanford Law School*, in *dirittocinese.com*, 8 aprile 2018.
Sul tema anche: C. LUMING – G. SUNI, *A Short Review of the Case Guidance System of the Chinese Judiciary*, in *asialaw.com*, 4 settembre 2019.

common law"[55]. Ad ogni modo, quel che interessa sottolineare in questa sede è che la pronuncia che stiamo per illustrare costituisce un paradigma valido per tutti i Giudici della Repubblica Popolare.

Il *Guiding-Case* n. 103 riguarda proprio un'ipotesi di «*sabotaging computer information system*». Una società che produce automezzi per l'edilizia dispone di un sistema di informazione satellitare, basato su servizi *GPS*, per monitorare i macchinari venduti a rate. Nei contratti stipulati dalla società ricorre, infatti, una clausola che autorizza il venditore a bloccare le attrezzature in caso di inadempimenti da parte dell'acquirente[56]. Quando il cliente ritarda o non effettua i pagamenti dovuti, l'automezzo riceve il comando di "blocco": può essere avviato, ma non è in grado di svolgere le proprie specifiche funzioni. Nel caso in analisi, gli imputati, dopo aver alterato i sistemi installati sull'automezzo, hanno utilizzato un *jammer GPS* per forzare il blocco di cinque autobotti vendute a rate dalla società. Ora, quanto più interessa in questa sede è che la Corte ha appurato, come primo punto, che il sistema di monitoraggio remoto dei veicoli, utilizzato dall'impresa, costituisce un sistema informatico[57]. Tale nozione viene, in particolare, ricostruita attraverso due elementi, uno strutturale e uno funzionale. In primo luogo, è possibile parlare di sistema informatico soltanto laddove siano individuate una serie di strutture tecnologiche interconnesse. Nel caso di specie, detto requisito è soddisfatto dalla piattaforma di monitoraggio remoto, dai terminali *GPS*, dai *controllers* e dai *display*. In secondo luogo, va analizzato il profilo funzionale del sistema informatico, vale a dire lo scopo e il normale funzionamento dello stesso. Tale requisito viene riconosciuto, nel caso di specie, nelle funzioni di trattamento automatico, archiviazione, trasmissione e riproduzione dei dati relativi alla funzione di controllo automatico degli equipaggiamenti.

La Corte Suprema del Popolo fornisce, quindi, una definizione di *computer information system* che associa la dimensione strutturale, diremmo *hardware*, alla *funzione* che queste componenti assolvono. La valorizzazione della *funzione* del sistema ci introduce all'analisi del bene giuridico tutelato dalle fattispecie di danneggiamento: vediamo in che termini.

5. L'oggetto di tutela: funzione e funzionamento del sistema informatico.

Le norme italiane poste a sanzione del danneggiamento informatico si trovano nel Capo I (Dei delitti contro il patrimonio mediante violenza alle cose o alle persone) del Titolo XIII (Dei delitti contro il patrimonio): tale collocazione suggerirebbe, dunque,

---

[55] J.E.H. LIMMER, *China's "new common law*, in *Willamette Journal of International Law and Dispute Resolution*, Vol. 21, No. 2, 2013, pp. 96-133. Un'interessante ricostruzione del sistema dei casi-guida si trova in *Chinese Common Law? Guiding Cases and Judicial Reform*, in *Harvard Law Review*, 10 giugno 2016.

[56] Nel testo originale, si legge: *Chūmài rén yǒu quán cǎiqǔ tíngjī, suǒ jī děng cuòshī" yǐ* (出卖人有权采取停机、锁机等措施"以).

[57] Nel testo originale, si legge: *Qǐyè de jīxiè yuǎnchéng jiānkòng xìtǒng shǔyú jìsuànjī xìnxī xìtǒng* (企业的机械远程监控系统属于计算机信息系统).

che si tratti di reati a tutela del patrimonio. È stata osservata, tuttavia, una differenza tra la fattispecie di danneggiamento "tradizionale" (art. 635 c. p.) e i reati di danneggiamento informatico. Nel primo caso, infatti, il bene giuridico tutelato è senz'altro da individuarsi nel patrimonio, in relazione sia alle cose mobili sia alle cose immobili[58]. Nelle fattispecie informatiche, invece, l'oggetto di tutela sarebbe costituito, più correttamente, dall'«integrità e dalla sicurezza dei sistemi e dei dati informatici»[59]. Gli artt. 635-*bis* e seguenti si caratterizzerebbero, dunque, per lasciare sullo sfondo la tutela patrimoniale[60]: la comparazione con l'ordinamento cinese rivela, tuttavia, come l'impostazione adottata dal Legislatore italiano conservi, invero, vari elementi di connotazione patrimonialistica[61].

In primo luogo, è utile analizzare le condotte tipiche descritte dalle norme dei due ordinamenti, per osservare come il codice italiano si attenga ad ipotesi strettamente legate ad una potenzialità lesiva o distruttiva. Tale aspetto risulta evidente dall'analisi dei verbi impiegati dagli artt. 635-*bis* e seguenti, che, escluso l'«alterare», individuano un campo semantico riconducibile all'idea del distruggere o cancellare («deteriora»; «sopprime»; «danneggiare»; «rendere inservibile»). Anche la condotta di alterazione, peraltro, potrebbe intendersi in senso "peggiorativo", considerato che si trova, nell'art. 635-*bis*, tra i verbi «cancella» e «sopprime»[62]. Si può dire, dunque, che le norme italiane tutelano l'integrità dei dati o programmi e la capacità di funzionamento[63] del sistema informatico.

Con soluzione differente, invece, l'art. 286 del codice cinese impiega le espressioni "cancellare, modificare, aggiungere e ostacolare il funzionamento"[64].

Ad una prima lettura, le condotte della fattispecie cinese sembrano rispecchiare quanto previsto dal codice italiano: dei quattro verbi elencati dalla norma cinese, tuttavia, soltanto il primo esprime esplicitamente l'idea di un danno in senso "distruttivo". Questo significa che l'intervento può essere, per configurare il reato in Cina, anche di tipo incrementativo o manipolativo, come nel caso dell'aggiunta (illecita) di dati ulteriori nel sistema, senza che tale attività comporti una vera interruzione del funzionamento del sistema. Ne discende che l'art. 286 del codice penale cinese non tutela tanto la capacità di funzionamento *tout court* del sistema informatico, quanto, piuttosto,

---

[58] In particolare, l'art. 635 tutelerebbe l'integrità e l'utilizzabilità della cosa: C. BACCAREDDA BOY, *Art. 635* (voce), in E. Dolcini – G. L. Gatta, *Codice Penale Commentato*, cit., 987; I. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante* cit., 204 ss.

[59] L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati, in Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004, 76.

[60] Ivi, 73.

[61] Vi è chi, peraltro, ritiene che il bene giuridico tutelato dalle norme in esame sia semplicemente il patrimonio: D. PAOLANTI, *Danneggiamento di informazioni, dati e programmi informatici dello Stato*, cit.

[62] È stato osservato che l'alterazione dovrebbe tradursi in una modificazione dei dati e programmi tale da «renderne impossibile il normale utilizzo per un lasso di tempo apprezzabile»: R. DE PONTI, *Art. 635*-bis (voce), in E. Dolcini – G. L. Gatta, *Codice Penale Commentato*, cit., 1016.

[63] Il riferimento è all'art. 615 *quinquies*.

[64] Cfr. S. WU, *Il codice penale della repubblica popolare cinese*, cit.,145. In lingua originale: *Duì jìsuànjī xìnxī xìtǒng gōngnéng jìnxíng shānchú, xiūgǎi, zēngjiā, gānrǎo* (对计算机信息系统功能进行删除、修改、增加、干扰).

la sua normale *funzione*. La legge penale cinese, del resto, si riferisce, testualmente, all'impossibilità per il sistema di funzionare normalmente[65].

Il *Guiding Case No. 104* (*People v. Li Sen, He Limin, Zhang Fengbo, et al.*) offre alcuni argomenti in questo senso, confermando come il bene giuridico tutelato dall'art. 286 del codice penale cinese vada propriamente individuato nel normale espletamento delle funzioni assegnate al sistema informatico. Il caso, deciso il 15 giugno del 2017, riguarda il sistema di monitoraggio della qualità dell'aria, che trasmette le informazioni al *China National Environmental Monitoring Center*. Secondo la ricostruzione operata dai Giudici cinesi, i soggetti imputati si sarebbero introdotti nella stazione di monitoraggio di *Chang'an* per compromettere i sistemi automatici di raccolta dei dati: lo scopo è stato raggiunto semplicemente ostruendo il campionatore con del filo di cotone. Tale operazione ha determinato numerose anomalie nei dati di monitoraggio e una complessiva distorsione delle informazioni riferibili a più periodi. Anche in questo caso, la Corte procede, in primo luogo, chiarendo che il sistema di monitoraggio dell'aria anzi descritto costituisce un sistema informatico[66]. Una volta definito tale aspetto essenziale, viene riconosciuto che la condotta posta in essere dai soggetti imputati costituisce il reato di danneggiamento informatico, riconoscendo, nel caso di specie, anche le gravi conseguenze richieste per l'applicazione dell'art. 286 del codice penale cinese[67]. Il *guiding case* permette di riflettere, dunque, sulla portata dell'evento previsto dalla norma dell'art. 286. Per certi versi, infatti, il sistema di monitoraggio dell'aria ha funzionato correttamente anche dopo l'intervento degli imputati, dal momento che non c'è stato un vero e proprio danneggiamento del circuito di elaborazione informatica del *computer*, ma, piuttosto, un intervento sui dati di *input*, che, proprio perché il sistema ha continuato ad operare, hanno dato informazioni distorte sulla qualità dell'aria. Ciò troverebbe conferma, peraltro, nel "punto di diritto" della sentenza[68], ove si precisa che il reato di *Sabotaging computer information system* si è configurato con l'ostruzione[69] dell'apparecchiatura, attraverso l'utilizzo di cotone.

Il fatto tipico della fattispecie cinese, insieme a quanto deciso nel *Guiding-case 104*, dimostra, dunque, che il bene giuridico tutelato dalla norma va individuato nella funzione che dovrebbe svolgere normalmente il sistema "attaccato": l'art. 286 sanziona,

---

[65] Art. 286 del codice penale cinese, primo comma. La traduzione ufficiale in lingua inglese si riferisce all'incapacità del sistema informatico «*to operate normally*». In lingua originale: *Zàochéng jìsuànjī xìnxī xìtǒng bùnéng zhèngcháng yùnxíng* (**造成**计算机信息系统不能正常运行). In particolare, la locuzione Zhèngcháng yùnxíng (**正常运行**) significa "funzionalità normale".

[66] Nel teso originale, si legge che: *Huánjìng zhí liàng jiāncè xìtǒng shǔyú jìsuànjī xìnxī xìtǒng* (环境质量监测系统属于计算机信息系统).

[67] Nel caso-guida, si specifica, infatti, che «l'interferenza provocata dagli imputati (nel caso, cinque soggetti) sul campionamento ha causato gravi conseguenze, che integrano il requisito delle "conseguenze gravi" stabilito dall'articolo 286 del codice penale» (*Wǔ bèigào rén gānrǎo cǎiyàng de xíngwéi zàochéngle yánzhòng hòuguǒ, fúhé xíngfǎ dì èrbǎi bāshíliù tiáo guīdìng de "hòuguǒ yánzhòng" yàojiàn*; **五被告人干**扰采样的行为造成了严重后果，符合刑法第二百八十六条规定的"**后果**严重"**要件**).

[68] Si tratta di una sezione chiamata *Cáipàn yàodiǎn* (裁判要点), letteralmente "punto del Giudice", nella quale si cristallizza la *ratio decidendi*.

[69] L'espressione utilizzata è *Dǔ* (堵) che, nella forma verbale, significa "bloccare" o "tappare": la condotta descritta non può, pertanto, considerarsi un attacco informatico in senso proprio.

pertanto, l'interferenza con il corretto svolgimento delle funzioni del sistema, tralasciando qualsiasi implicazione patrimonialistica[70].

Simili argomenti non possono riferirsi, invece, alle quattro fattispecie dell'ordinamento italiano. Come si è già detto, infatti, le condotte tipiche descritte dal codice penale implicano un intervento che si risolva, in definitiva, in un malfunzionamento, peraltro grave[71], dell'elaboratore. La differenza tra i due ordinamenti si coglie, in particolare, ipotizzando il caso dell'aggiunta illecita di dati al sistema, tale da provocare una distorsione nei risultati dell'elaborazione informatica. Una simile ipotesi può integrare, in Cina, il delitto di danneggiamento informatico, poiché rientra nel caso di chi, «compiendo operazioni di aggiunzione»[72], impedisce al sistema di operare normalmente. Nell'ordinamento italiano «l'introduzione di dati, informazioni o programmi» è espressamente contemplata dall'art. 635-*quater*: tuttavia, si tratta di una particolare modalità commissiva il cui esito deve essere comunque quello di «distruggere, danneggiare, rendere inservibile o ostacolare gravemente il funzionamento del sistema informatico».

In questo senso, il danneggiamento informatico presenta ancora, in Italia, i tratti di una fattispecie ispirata alla difesa del patrimonio, dal momento che la tutela accordata dagli artt. 635-*bis* e seguenti del codice penale sembra riferirsi ai dati e sistemi informatici intesi più come *res alicuius* che non come reti di informazioni e funzioni. Quanto appena detto trova conferma osservando che i dati e i sistemi menzionati dagli artt. 635-*bis* e *quater* debbono essere «altrui». Il requisito dell'altruità mal si concilia con la natura dematerializzata dei dati informatici[73], risultando, in definitiva, un retaggio mutuato dalle fattispecie di danneggiamento tradizionale. Nell'ordinamento italiano, allora, l'oggetto di tutela individuato dagli artt. 635-*bis* e seguenti va riconosciuto sì nell'integrità e sicurezza dei sistemi informatici, ma quest'ultimi sono considerati come beni a rilevanza patrimoniale: per questo motivo, la tutela si focalizza sulla capacità di funzionamento dei sistemi stessi.

6. Il rapporto tra invio di virus e danneggiamento informatico.

La comparazione tra Italia e Cina permette di approfondire un ultimo aspetto. Il danneggiamento di dati e sistemi informatici è spesso l'esito dell'impiego dei c.d. *malware*: in entrambi gli ordinamenti, si prevedono fattispecie penali a sanzione della creazione e diffusione di virus informatici.

---

[70] Nel caso-guida analizzato, del resto, non viene riconosciuto un danneggiamento del sistema informatico, ma un'interferenza con lo stesso: l'espressione impiegata dal codice cinese e richiamata nella sentenza è *Gānrǎo* (干扰), che significa propriamente "turbare", "interferire".

[71] Ai sensi dell'art. 635-*quater* c.p., si richiede, tra le altre condotte, che il soggetto agente ostacoli «gravemente» il funzionamento del sistema.

[72] S. WU, *Il codice penale della repubblica popolare cinese*, cit., 145.

[73] A. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, cit., 781.

Il quadro sanzionatorio previsto dal codice penale italiano è l'esito della riforma introdotta dalla L. 48/2008. L'art. 615-*quinquies*, quale riformato da questa novella, punisce chiunque, allo scopo di danneggiare illecitamente un sistema informatico o i dati ad esso pertinenti, ovvero di favorire l'interruzione o l'alterazione del suo funzionamento, si procura, produce o diffonde apparecchiature, dispositivi o programmi informatici.

La tecnica di *drafting* adottata dal Legislatore si caratterizza, invero, per l'impiego di un ampio novero di condotte tipiche, per le quali si pongono due diversi ordini di criticità. In primo luogo, la distinzione, sul piano semantico, delle espressioni impiegate dall'art. 615-*quinquies* non risulta sempre agevole. Vengono impiegati, ad esempio, i termini, apparentemente equivalenti, «comunica», «consegna» e «diffonde»: la differenza tra le locuzioni appena richiamate si potrebbe ricostruire nel senso che la diffusione presuppone una condotta rivolta ad un numero indeterminato di destinatari, mentre, nel caso di consegna o comunicazione, i destinatari sarebbero individuati e specifici[74].

In secondo luogo, è stato evidenziato come alcune delle condotte perseguite dalla norma in esame comportino una (pericolosa) anticipazione della soglia di rilevanza penale, già piuttosto arretrata, trattandosi di reato di pericolo. Si possono leggere, in questo senso, le condotte tipiche del procurarsi o importare un programma dannoso: tali previsioni si rivelano particolarmente problematiche, se si considera che risultano prodromiche non soltanto alla commissione del danneggiamento informatico, ma anche alla stessa diffusione di virus informatici[75].

Spostando l'attenzione all'ordinamento cinese, si osserva come la norma di riferimento per la sanzione dei virus informatici sia ancora l'art. 286. Quanto interessa è, in questo caso, il terzo comma della fattispecie, con il quale è punito «chiunque, intenzionalmente, producendo o diffondendo virus informatici o altri programmi distruttivi, interrompe il funzionamento del sistema informatico o telematico»[76].

Il carico sanzionatorio è, ancora una volta, il medesimo visto per il primo comma dell'art. 286. Le condotte tipiche sono in parte sovrapponibili a quelle viste con l'articolo 615-*quinquies* italiano, benché vi sia una differenza importante: il codice penale cinese non persegue l'attività prodromica di chi si procura il programma dannoso[77].

Ciò premesso, si osserva, invero, come la struttura del reato sia affatto diversa nei due ordinamenti. La norma cinese richiede che i programmi creati o inviati siano

---

[74] L. PICOTTI, voce *Reati informatici*, in *Enciclopedia giuridica Treccani*, 2000, 19; R. DE PONTI, *Art. 635*-bis (voce), in E. Dolcini – G. L. Gatta, *Codice Penale Commentato*, 625-626; V. DESTITO, Digesto, cit., 749.

[75] A.C. AMATO MANGIAMELI – G. SARACENI, *I reati informatici. Elementi di teoria generale e principiali figure criminose*, 2015, Torino, 70 ss.

[76] La traduzione italiana è tratta da S. WU, *Il codice penale della repubblica popolare cinese*, cit.,145.

[77] Va precisato, tuttavia, che il codice penale cinese prevede, all'art. 22, un particolare istituto di diritto penale generale, il c.d. reato preparato: «È reato preparato predisporre i mezzi o porre le condizioni al fine di commettere un reato». Non si può escludere, pertanto, che la condotta di chi si procura o produce un malware risulti comunque punibile come forma di preparazione del reato previsto dall'art. 286 del codice. Sulla preparazione del crimine, alcune considerazioni in: S. VINCIGUERRA, *Impressioni di un penalista italiano*, cit., 47.

«distruttivi»[78]: i codici informatici dovranno, pertanto, essere intrinsecamente o almeno potenzialmente dannosi. Al contrario, nella fattispecie italiana la carica lesiva del fatto tipico dipende unicamente dall'elemento soggettivo[79]: la condotta è, infatti, perpetrata «allo scopo di danneggiare illecitamente un sistema informatico». Il danneggiamento del *computer system* non rileva, dunque, come potenzialità "tecnica" del programma, ma soltanto come finalità cui è preordinata la condotta del soggetto agente[80]. Se il Legislatore avesse voluto, infatti, richiedere certe caratteristiche del *software*-virus, avrebbe potuto ricorrere all'espressione "apparecchiature atte a", come previsto, ad esempio, dall'art. 617-*quinquies*. A ben vedere, il riferimento alla pericolosità del codice informatico era presente nella versione originaria dell'art. 615-*quinquies*, ove si menzionava «il programma informatico (…) avente per scopo o per effetto il danneggiamento di un sistema». Nella nuova formulazione della fattispecie, invece, la carica offensiva della condotta incriminata emerge soltanto sul piano dell'elemento soggettivo, tanto che, escludendo l'inciso che enuncia il dolo specifico, risulterebbe paradossalmente imputabile «Chiunque (…) si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici».

Da questa prima analisi, emergono alcune delle potenziali criticità applicative della norma italiana: ci si potrebbe domandare, ad esempio, se sia penalmente rilevante la trasmissione di programmi o applicazioni lecite e diffuse sul mercato, se effettuata allo scopo di provocare l'interruzione del sistema altrui, come nel caso di trasmissione di un *software* notoriamente "pesante" verso un elaboratore, al solo fine di provocarne il rallentamento[81]. Allo stesso modo, bisognerebbe chiedersi se ricorra il delitto di cui all'art. 615-*quinquies* nel caso di diffusione, con la descritta finalità, di un programma che si riveli del tutto innocuo.

Si tratta di un'ipotesi che ci porta, sotto certi profili, ad affrontare il tema del tentativo. L'art. 615-*quinquies* costituisce un reato di pericolo presunto: la configurabilità della fattispecie tentata è, pertanto, discussa, dal momento che esisterebbe il rischio di rendere punibile il c.d. "pericolo di un pericolo"[82]. L'ipotesi tentata risulta, in ogni caso, difficile da configurare, considerando l'ampiezza della fattispecie in esame: con la mera trasmissione di un *malware*, senza che ne consegua alcun danno, il delitto risulterebbe,

---

[78] La norma, in lingua originale, si riferisce a «programmi distruttivi come i virus informatici»: *Chuánbò jìsuànjī bìngdú děng pòhuài xìng chéngxù* (传播计算机病毒等破坏性程序).

[79] A. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in A. Cadoppi, S. Canestrari, A. MANNA, *Cybercrime*, 2019, Milano, 811 ss.

[80] Alcuni Autori, tuttavia, ritengono che il principio di offensività imponga di accertare che gli strumenti siano «dotati di una effettiva potenzialità offensiva»: R. DE PONTI, *Art. 635*-bis (voce), in E. Dolcini – G. L. Gatta, *Codice Penale Commentato*, cit., 623. Tale interpretazione è senz'altro da preferire, ma il dato normativo, come si dirà, non sembra offrire elementi che impongano una valutazione sulla nocività intrinseca dei programmi utilizzati dal soggetto agente.

[81] Considerazioni simili in A. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in *Cybercrime*, cit., 703.

[82] Sul punto: V. DESTITO, *Digesto*, cit., 751; A. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in *Cybercrime*, cit.,816-817.

infatti, già consumato. La fattispecie tentata si potrebbe verificare, allora, nel caso di fallimento della procedura di diffusione, come nell'ipotesi di invio non riuscito dell'*e-mail* contenente il virus, oppure in caso di fallimento nella creazione del *malware*: tuttavia, la soglia di rilevanza penale si rivelerebbe, in questi casi, irragionevolmente arretrata. Un ulteriore dubbio applicativo attiene all'ipotesi di diffusione di un virus effettuata, tuttavia, nella consapevolezza che la minaccia sarà facilmente e prontamente neutralizzata da *software* antivirus, senza che ne derivi alcun disturbo per l'elaboratore. Una fattispecie, questa, che delineandosi, probabilmente, come forma di dolo eventuale, rivela un possibile *vulnus* nella tutela apprestata dall'art. 615-*quinquies*.

Se si considera la fattispecie cinese si nota come sia richiesto il verificarsi di un evento, consistente nel malfunzionamento del sistema attaccato. Tale impostazione lascia un margine più definito per l'ipotesi del delitto tentato, che il codice penale cinese disciplina all'art. 23: «È reato tentato iniziare a commettere un reato ma senza successo a cagione di fattori non voluti dal reo»[83]. Nel caso del terzo comma dell'art. 286, infatti, la trasmissione di un programma dannoso senza conseguenze per il sistema informatico costituisce l'inizio della commissione di un crimine che, tuttavia, non può dirsi compiuto[84].

L'analisi del tentativo mette in luce un aspetto importante della norma cinese: si tratta, anche in questo caso, di una fattispecie di vero e proprio danneggiamento informatico. Se non avviene il danneggiamento, infatti, il delitto è solo tentato, dovendosi applicare, in base all'art. 23, secondo comma, una pena diversa, più "leggera", o un carico sanzionatorio mitigato[85].

In Cina, il confine tra invio di virus e danneggiamento informatico si può sintetizzare in questi termini: tra il primo e il terzo comma dell'art. 286 vi sarebbe un rapporto di genere a specie, dove il secondo rappresenta una particolare modalità commissiva del primo. Anzi, le due norme si riferirebbero a diverse forme dello stesso crimine, con l'unica differenza che, nel terzo comma, l'attività illecita può essere commessa «*through the network*»[86].

La norma cinese configura un reato di evento a condotta vincolata. È un aspetto essenziale nel raffronto tra i due ordinamenti: nella fattispecie cinese assume centralità, per l'applicazione della norma, non tanto la trasmissione del virus, quanto, piuttosto, il danneggiamento (in senso lato) del sistema informatico. Tanto è vero, che il semplice *spreading* di un *malware* non sembrerebbe integrare il reato in esame, richiedendosi che tale condotta provochi effettivamente un malfunzionamento del sistema "infettato".

---

[83] La traduzione italiana è tratta da S. WU, *Il codice penale della repubblica popolare cinese*, cit., 145.

[84] Per un'approfondita ricostruzione sulla "pericolosità dell'azione" e l'"efficacia causale dell'azione tentata": L. HANYUE, *Rationale for Punishing Criminal Attempt via the Functional Danger Concept* (*Wèisuì chǔfá gēnjù de gōngnéng xìng wéixiǎn lùnzhèng*; **未遂**处罚根据的功能性危险论证), in *Zhōngwài fǎxué* (**中外法学**), n. 6, 2019. Per alcune considerazioni sul delitto tentato in Cina: X. XIAOHUI, *On the Beginning Point of Attempt in Criminal Law*, in *Héběi fǎxué* (**河北法学**), n. 10, 2008.

[85] Nel testo in lingua originale: *Duìyú wèisuì fàn, kěyǐ bǐzhào jìsuì fàn cóng qīng huòzhě jiǎnqīng chǔfá* (对于未遂犯，可以比照既遂犯从轻或者减轻处罚). Si noti, anche in questo caso, come la formulazione della norma lasci ampi margini discrezionali all'autorità giudicante.

[86] P. YONG, *Comparative research*, cit., 2.

Una simile impostazione si riflette, in definitiva, sul ruolo svolto dal tipo di programma creato o diffuso: non solo il programma doveva essere, come visto, preordinato a causare un malfunzionamento, ma detto danneggiamento deve essersi effettivamente verificato, altrimenti il reato non è consumato.

Va rilevato, in ogni caso, che i virus informatici sono oggetto, in Cina, di un poderoso *corpus* di norme extra-penali, che perseguono, con sanzioni amministrative[87], anche la mera produzione e diffusione di *malware*: si considerino, in questo senso, l'art. 6 delle misure amministrative per la prevenzione e il controllo dei virus informatici[88] e gli artt. 22 e 25 della successiva *Cybersecurity Law*[89].

Più complessa è la ricostruzione dei confini che intercorrono, nel sistema italiano, tra le fattispecie di cui agli artt. 635-*bis* ss. e l'art. 615-*quinquies*. Quest'ultimo costituisce, infatti, una fattispecie di pericolo, sicché, come si è detto, il delitto si configura indipendentemente dal verificarsi di un danno. È possibile osservare che l'art. 615-*quinquies* e gli artt. 635-*bis* e seguenti tutelano il medesimo bene giuridico[90] (la sicurezza e l'integrità dei sistemi informatici) essendo l'una fattispecie prodromica rispetto alle altre. La trasmissione di virus informatici potrebbe costituire antefatto non punibile rispetto al delitto di danneggiamento informatico, giacché quest'ultimo sanziona il concretizzarsi del medesimo pericolo individuato dall'art. 615-*quinquies*: considerando l'identità dell'oggetto di tutela, in simili ipotesi troverebbero applicazione gli artt. 635-

---

[87] Si deve considerare, peraltro, che, nell'ordinamento cinese, la differenza tra sanzione penale e sanzione amministrativa si rivela, per certi versi, più formale che sostanziale, dal momento che anche la condanna amministrativa può comportare forme di reclusione. È sufficiente, in questo senso, leggere il testo dell'art. 63 della *Cybersecurity Law*, che, nel sanzionare varie condotte pericolose per la sicurezza della rete, prevede che l'autorità competente «*where circumstances are serious, shall impose between 5 and 15 days detention*». Il testo integrale della legge è disponibile sul portale *chinacopyrightandmedia*, all'URL: https://chinacopyrightandmedia.wordpress.com/2016/11/02/cybersecurity-law-of-the-peoples-republic-of-china-third-reading-draft/.

[88] Le "Misure amministrative per la prevenzione e il controllo dei virus informatici" sono state adottate il 30 marzo 2000 dall'Ufficio del Ministro della Pubblica Sicurezza: *Jìsuànjī bìngdú fángzhì guǎnlǐ bànfǎ" yǐjīng 2000 nián 3 yuè 30 rì gōng'ān bù bùzhǎng bàngōng huìyì tōngguò, xiàn yǔ fābù shīxíng* (计算机病毒防治管理办法 已经2000年3月30日公安部部长办公会议通过，现予发布施行). Il Documento prevede il divieto generale di creazione di virus, al quale seguono dei più specifici divieti di diffusione di *malware*: tra le condotte menzionate e, dunque, proibite dall'art. 6, sono elencate la fornitura di *file*, *software* e supporti contenenti virus informatici (art. 6, n. 2), la vendita, il noleggio e la distribuzione di supporti contenenti virus informatici (art. 6, n. 3).

[89] Si tratta della *Cybersecurity Law of the People's Repubblic of China*, approvata il 7 novembre 2016 ed in vigore dal 2017. L'art. 22 prevede, nella traduzione inglese, che: «*Providers of network products and services must not install malicious programs; when discovering that their products and services have security flaws or vulnerabilities, they shall immediately adopt remedial measures, and follow provisions to promptly inform users and report to the competent departments*». L'art. 60 dispone sanzioni pecuniarie per la violazione dell'art. 22, nel caso in cui siano installati programmi dannosi. È possibili osservare come le norme appena richiamate si rivolgano ai *Network Operators*: l'impostazione della *Cybersecurity Law* prevede, infatti, il coinvolgimento e la responsabilizzazione dei *provider* per implementare la sicurezza informatica, costruendo il c.d. *MLPS* (*multi-level protection system*) introdotto dall'art. 21 della stessa legge.

[90] L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. Picotti (a cura di), *Il diritto penale dell'informatica all'epoca di internet*, 2004, Padova, 70-75; R. DE PONTI, *Art. 635*-bis (voce), in E. Dolcini – G. L. Gatta, *Codice Penale Commentato*, cit., 622.

bis e *quater*, stando al criterio del maggiore minimo edittale. Il reato previsto dall'art. 615-*quinquies* sarebbe, dunque, assorbito nelle fattispecie di danneggiamento[91] tutte le volte in cui il programma dannoso determina l'interruzione del funzionamento del sistema informatico.

È evidente, insomma, come l'applicazione dei reati di danneggiamento oppure dell'art. 615-*quinquies* dipenda dalla sussistenza o meno di un danno al sistema informatico: possono, tuttavia, verificarsi ipotesi incerte, in cui non appare semplice stabilire se l'elaboratore sia danneggiato, come nel caso di un virus latente in un *PC* che, connesso alla rete, provoca la diffusione automatica del *malware* verso altri *computer*[92]. Un'ulteriore criticità si evidenzia nel rapporto tra il tentato danneggiamento informatico e l'invio di *malware*: in tali ipotesi, potrebbe prevalere quest'ultimo, in forza del principio di specialità[93].

La matassa diventa ancor più inestricabile quando si considera il confine tra l'art. 615-*quinquies* e i reati previsti dagli artt. 635-*ter* e 635-*quinquies*: l'invio di virus ad un sistema informatico di pubblica utilità potrebbe, infatti, costituire un fatto diretto a distruggere i dati o i sistemi utilizzati dallo Stato, come previsto dalle particolari fattispecie di danneggiamento anzi richiamate. Ora, considerando che, in dette ipotesi, l'effettivo danneggiamento del sistema costituisce, ai sensi del secondo comma di entrambe le norme, una circostanza aggravante, è ragionevole ritenere che l'anticipazione di tutela configurata dal primo comma degli artt. 635-*ter* e 635-*quinquies* si ponga in rapporto di specialità rispetto al più generico reato di pericolo previsto dall'art. 615-*quinquies*.

La ricostruzione operata dimostra come la maggiore ampiezza di tutela prevista dal Legislatore italiano nel caso dei virus informatici si risolva in un'incertezza di fondo circa i confini applicativi delle fattispecie penali, restituendo un quadro sanzionatorio per certi versi più complesso e imprevedibile rispetto all'impostazione vista per l'ordinamento cinese.

7. Conclusioni.

La comparazione tra Italia e Cina consente di svolgere alcune considerazioni conclusive.

Sia il diritto italiano sia il diritto cinese considerano il sistema informatico meritevole di tutela penale. Esiste, infatti, una tendenziale convergenza dei due sistemi penali nel campo dei reati informatici[94] ed, in particolare, nelle fattispecie di danneggiamento.

---

[91] A. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in *Cybercrime*, cit., 817.

[92] Un esempio analogo è riportato in V. DESTITO, *Digesto*, cit., 750.

[93] Così V. DESTITO, ivi, 751.

[94] Tale aspetto risulta anche dalla comparazione di altre fattispecie di diritto penale dell'informatica. Nel codice cinese si trovano norme comparabili con gli articoli del codice italiano in tema di accesso abusivo ad un sistema informatico (cui corrisponde l'art. 285 del codice penale cinese); di tutela delle comunicazioni

Tale aspetto può sorprendere. L'ordinamento cinese, infatti, non aderisce a quelle fonti di diritto convenzionale che hanno portato, in Italia, all'introduzione dei reati di danneggiamento informatico. E di certo, Italia e Cina non condividono il medesimo percorso storico-culturale, né la medesima tradizione giuridica o il medesimo *background* costituzionale. Da dove nasce, allora, l'impostazione comune dei due Paesi? La più autorevole dottrina italiana e cinese è concorde nel riconoscere il carattere transnazionale e aterritoriale del fenomeno informatico[95], che determina, in definitiva, scelte di politica criminale comuni ai diversi ordinamenti giuridici. Come si è visto, ad un'analisi attenta delle fattispecie, emergono invero delle differenze di fondo: è diversa la *ratio* alla base dello sdoppiamento di norme, è diversa la concezione di tutela del sistema informatico ed è diversa la tecnica legislativa. È proprio questo differente punto di partenza, tuttavia, che permette di valorizzare, ancora di più, la relativa convergenza delle fattispecie analizzate in materia di *cybercrime*. L'estensione globale delle funzioni dell'informatica e della rete pongono, infatti, le medesime sfide e criticità, con le quali il diritto deve confrontarsi. Un aspetto, questo, dimostrato dall'importante ruolo svolto nella regolamentazione del cyberspazio dalle fonti sovranazionali, alle quali l'ordinamento cinese rivolge grande attenzione. Da questo punto di vista, seguendo l'indicazione di Rodolfo Sacco, per il quale il comparatista è «sommamente interessato a tutte le fonti indirette che condizionano l'intero funzionamento del diritto»[96], si può dire che benché manchi un'adesione formale della Cina alla Convenzione di Budapest, quest'ultima entra a far parte del diritto penale dell'informatica cinese come strumento di approfondimento accademico e come parametro di analisi delle norme rilevanti[97].

La comparazione Italia-Cina mostra, dunque, che i fenomeni digitali, essenzialmente globali e transnazionali, modellano e conformano il diritto dei diversi Paesi, imponendo al giurista di oggi di volgere il proprio sguardo oltre i confini dell'ordinamento nazionale.

Questa ricerca consente anche un'altra riflessione. Abbiamo confrontato due sistemi penali profondamente diversi. L'avverbio "profondamente" è d'obbligo: la Costituzione della Repubblica Popolare Cinese non riconosce il principio di divisione dei poteri, sicché, come si è visto, anche il principio di legalità dell'ordinamento penale

---

(cui corrisponde l'art. 252 del codice penale cinese); di frode informatica, cui possono avvicinarsi gli artt. 266 e 287 del codice penale cinese, così come interpretati dalla Corte Suprema del Popolo con l'opinione N. 32, del 20 dicembre 2016.

[95] Si considerino, fra tutti: G. PASCUZZI, *Il diritto dell'era digitale*, cit. *passim* (in particolare, 324 ss); F. CORONA, *I reati informatici*, in M. Iaselli (a cura di), *Diritto e nuove tecnologie, Prontuario giuridico-informatico*, 2016, Milano, 381; P. YONG, *New China Criminal Legislations in the Progress of Harmonization of Criminal Legislation against Cybercrime*, in *coe.int*, 2011.

[96] R. SACCO – P. ROSSI, *Introduzione al Diritto Comparato*, in R. Sacco (diretto da), *Trattato di diritto comparato*, 2015 (VI Ediz.), Milano, 13.

[97] Lo dimostra, in particolare, il contributo di Zhang Jin e Shen Hua, i quali esaminano e confrontano l'art. 615 ter del codice penale italiano con il reato di *Ausspähen von Daten* (spionaggio di dati) previsto dalla Sezione 202 dello *Strafgesetzbuch* tedesco, dei quali viene fornita una traduzione integrale in cinese: gli Autori cinesi analizzano la differente attuazione dell'obbligo posto dall'art. 3 della Convenzione di Budapest negli ordinamenti italiano e tedesco. J. ZHANG e S. HUA, *On International Cooperation in AntiComputer Crime Measures and Its Legislation in Relative Countries*, in Zhèngzhì yǔ fǎlǜ (政治与法律), 2004.

ne risulta più debole. Poste queste premesse, ci si poteva aspettare che il confronto con il nostro ordinamento fosse impari: i princìpi sanciti dagli artt. 25 e 27 della Costituzione italiana impongono che la legge penale sia tassativa, certa e sufficientemente determinata.

A ben vedere, però, le caratteristiche innovative della dimensione digitale determinano, in tutti i sistemi, problemi di corrispondenza tra la fattispecie penale e l'attività illecita da perseguire[98]. Il *cybercrime* pone, in altre parole, un problema di tipicità. Ebbene, la verifica condotta con questa ricerca permette di osservare come a queste nuove sollecitazioni il diritto dei due Paesi reagisca in modo analogo, simmetrico, indipendentemente dalla diversa cornice formale di valori costituzionali. In particolare, si possono evidenziare due diversi atteggiamenti.

In primo luogo, le ipotesi delittuose possono essere ritagliate su modelli specifici di *cybercrime*. In questi casi, può accadere che il fatto tipico descritto dalla norma non riesca a coprire tutte le forme di *hacking* possibili: il rischio è, dunque, quello di creare ingiustificati vuoti di tutela. Questa impostazione si coglie, nell'ordinamento cinese, con riferimento alla lesione di quei dati che non siano parte di un sistema informatico: l'art. 286 del codice penale cinese non è in grado di perseguire simili condotte. Un analogo *vulnus* si verifica nell'ordinamento italiano con riferimento agli artt. 635-*bis* e seguenti, inidonei a sanzionare la mera manomissione o aggiunta di dati, che non comprometta gravemente il funzionamento del sistema.

Per evitare di configurare reati eccessivamente "selettivi", la legislazione penale può allora ricorrere a fattispecie particolarmente ampie e tendenzialmente onnicomprensive, come reazione alla vastità e alla mutevolezza del crimine informatico: il rischio, in questo caso, è però quello di una sostanziale imprevedibilità dei confini della responsabilità penale. Valgano in questo senso le criticità evidenziate per il rapporto tra il danneggiamento informatico e il delitto (consumato o tentato) previsto dall'art. 615-*quinquies* c. p. Nel sistema penale cinese, può ascriversi a questa tendenza il ricorrere, anche in materia di *cybercrime*, ad espressioni vaghe, dai confini incerti.

Ecco il punto: la legge penale di un sistema basato sui princìpi di legalità, tassatività e determinatezza presenta le medesime criticità applicative della legge penale di un Paese che disconosce la divisione dei poteri, accogliendo una concezione debole del principio di legalità. Ci si potrebbe domandare come ciò sia possibile: due considerazioni chiariscono tale aspetto.

Si sono più volte evidenziati i problemi che affliggono le fattispecie penali italiane. L'attuale assetto legislativo è l'esito di un'importazione acritica del testo della Convenzione di Budapest: un "copia e incolla" che ha conferito alla fonte convenzionale il rango di fattispecie punitiva nazionale. Tale impostazione dà luogo a serie difficoltà applicative e di coordinamento normativo, sicché, nonostante la previsione delle massime garanzie a livello costituzionale, la fonte primaria non può dirsi soddisfacente.

---

[98] Le difficoltà di inquadramento del crimine informatico si riscontrano, del resto, anche nell'analisi criminologica, atteso che gli idealtipi elaborati, in questo campo, per classificare il *cybercrime* risulterebbero poco riconoscibili nella realtà empirica. Per un approfondimento in questo senso: G. MICILOTTI, *La Cybercriminalità*, in A. Balloni, R. Bisi, R. Sette, *Criminologia applicata*, 2019, Milano, 324ss.

Sotto altro aspetto, si è più volte sottolineato come dalla Costituzione cinese discenda un sistema penale meno garantista. Ciò è vero. Tuttavia non si può trascurare che il codice del 1997 ha rappresentato un "grande balzo in avanti" per il diritto penale cinese[99]. Rispetto al precedente codice del 1979[100], infatti, sono stati introdotti sia il divieto di analogia[101] sia il riconoscimento formale del principio di legalità[102] (la cui portata è, comunque, relativa). In questo senso, anche la disciplina dei reati informatici risente del processo di sviluppo di nuove e più forti garanzie nel sistema penale cinese, conferendo alla fattispecie un'impostazione più simile a quella degli ordinamenti occidentali e delle fonti internazionali. Certo, scopo della comparazione non è quello di esprimere una «*valutazione, positiva o negativa, delle istituzioni* altrui»[103]. Di questo chi scrive è fermamente convinto. Altrettanto certo è, però, che un diritto penale moderno non può prescindere dal riconoscimento di principi garantistici ineludibili: primo fra tutti, la certezza del diritto[104]. In questi termini, lo sviluppo di un diritto penale certo e prevedibile è una strada che la Cina di oggi ha già intrapreso e ha il dovere di proseguire.

In questa direzione e nell'auspicata prospettiva di riforma del danneggiamento informatico italiano, le più autorevoli Istituzioni internazionali, cui sia l'Italia sia la Cina aderiscono, potrebbero cogliere ciò che accomuna gli ordinamenti studiati, per guidare un processo di ripensamento del diritto penale dell'informatica[105].

---

[99] Sul tema: I CARDILLO, *Lo sviluppo del diritto penale cinese dalla fondazione della repubblica popolare ad oggi*, in *Diritto Penale XXI Secolo*, Anno XVII, 2018.

[100] Per alcune autorevoli considerazioni sul primo codice penale promulgato dalla Repubblica Popolare Cinese e sull'intenso dibattito della dottrina cinese circa l'opportunità di riconoscere o meno il principio della presunzione di innocenza: F. STELLA, *Giustizia e Modernità. La protezione dell'innocente e la tutela delle vittime*, Milano, 2003, pp. 77-78.

[101] Il divieto di analogia non è, però, sancito da una norma costituzionale. Sul punto: L. PICOTTI, *Offensività ed elemento soggettivo del reato nel codice penale della repubblica popolare cinese*, in *Diritto Penale XXI Secolo*, Anno IX, 2010, p. 54.

[102] L'art. 3 del codice penale cinese prevede che "qualunque fatto che sia espressamente previsto come reato dalla legge va condannato e punito, qualunque fatto che non sia espressamente previsto come reato dalla legge non va né condannato né punito".

[103] R. SACCO – P. ROSSI, *Introduzione al diritto comparato*, cit., pp. 4-5.

[104] M. DONINI, *Disposizione e norma nell'ermeneutica penale contemporanea*, in ID., Europeismo giudiziario e scienza penale. Dalla dogmatica classica alla giurisprudenza-fonte, Giuffrè, 2011, 63 ss., 92 ss.

[105] L'auspicio è condiviso dall'illustre giurista cinese, più volte citato in questa ricerca, P. YONG, in *New China Criminal Legislations in the Progress of Harmonization of Criminal Legislation against Cybercrime*, cit., 6.