CONVEGNI

FRANCESCO CAMPLANI

Locus commissi delicti, norme di collegamento e reati informatici a soggetto passivo indeterminato*

La determinazione del *locus commissi delicti*, nell'ambito dei reati informatici, è questione di grande complessità. Le condotte e gli eventi dei reati informatici consistono essenzialmente nell'emanazione o nella captazione in una serie di impulsi elettronici che si muovono lungo piattaforme immateriali accessibili indifferentemente da qualsiasi persona in qualsiasi luogo del mondo e nei relativi effetti, nel contesto di una rete acefala e priva di un governo centrale: ne consegue la facilità con cui il reato informatico assuma una dimensione transnazionale, che richiede il ricorso a norme di collegamento territoriale, e la complessità tecnica della localizzazione delle stesse. Il problema della collocazione del *locus* si risolve più agevolmente quando sia individuabile il soggetto passivo del reato, collocando l'evento nel luogo in cui si verifichi l'evento lesivo. Diventa di più ardua risoluzione quando il soggetto passivo sia indeterminato, come generalmente succede in relazione alle fattispecie di pericolo, soprattutto se astratto.
Il contributo si propone di porre in evidenza le specificità di tali fattispecie, soprattutto negli ordinamenti italiano e tedesco, commentando le possibili soluzioni volte a individuare il *locus commissi delicti*.

Locus commissi delicti, conflict-of-law rules and computer crimes with an undetermined passive subject

The determination of the *locus commissi delicti*, in the context of computer crimes, is a matter of great complexity. The behaviours and events of cybercrime consist basically in emanating or capturing a series of electronic impulses - and their related effects - that move along with immaterial platforms, accessible without restrictions from any person anywhere in the world. The general context is a leaderless network without any central authority. Consequently, it is easy for the cybercrime to assume a transnational dimension; the inquiry about the localisation of those facts presents a relevant technical complexity. This requires the use of jurisdiction rules. However, they are not always suitable for the contrast to cybercrime: the problem related to the *locus* can be easily solved when the offended is identifiable – then the *locus* can be identified in the place of the offence. It becomes harder when the offended is indeterminate, as it generally happens concerning the case of dangerous offence, especially in the case of abstract danger crimes.
The present contribution aims at focusing the specificities of those cases, especially in the Italian and German law systems. At the end, several solutions to identify the *locus commissi delicti* are going to be analysed.

* Il presente lavoro costituisce un ampliamento ed aggiornamento della relazione dal medesimo titolo tenuta presso il *Siracusa Institute* il 29 novembre 2018, in occasione del IX Corso di formazione interdottorale di diritto e procedura penale "Giuliano Vassalli" per Dottorandi e Dottori di ricerca. Il tema dell'evento è stato "Nuove frontiere tecnologiche e sistema penale. Sicurezza informatica, strumenti di repressione e tecniche di prevenzione".

crimini di internet. 5.2. La proposta dell'applicazione al diritto penale della soluzione di cui alla Direttiva UE in materia di *E-Commerce*. 5.3. Soluzioni a breve termine per gli ordinamenti interni. La parte generale del diritto penale. 5.4. (segue) I *cybercrimes* della parte speciale ed il corretto recepimento della Convenzione di Budapest. Il modello tedesco. 6. Conclusioni.

1. *Considerazioni introduttive*. Uno dei problemi più evidenti posti dallo sviluppo delle tecnologie informatiche e, in particolare, di internet, è senz'altro lo sviluppo di un settore di criminalità transnazionale che si muove in un "luogo" la cui consistenza fisica è, per definizione, evanescente.
Internet può essere definito come una rete di messaggi elettronici che si muovono attraverso degli snodi contenenti basi di dati, i *server*, e attraverso altri elaboratori elettronici. Tali messaggi elettronici sono accessibili tramite *software* di interfaccia, i *browser*, che rappresentano nell'esperienza comune il terminale più concreto cui la generalità degli utenti si approccia. *Server* ed elaboratori elettronici comuni assumono anche la funzione statica di depositi in cui i dati veicolati dai messaggi elettronici vengono catalogati in "fascicoli", i *files*[1].

[1] Un testo dal quale attingere definizioni volte a dare corpo al concetto di *Internet*, scritto con un linguaggio accessibile anche agli esperti di scienze umane e sociali, si trova in da BATINI, PERNICI, SANTUCCI, ARDAGNA, FUGINI, PLEBANI, *Sistemi informatici*, Roma, 2006, specialmente la *Premessa* e l'*Introduzione* di cui alle pp. 9 e ss.
La dottrina giuridica ha dimostrato una sensibilità al tema che si è mossa di pari passo con la "dematerializzazione" delle reti attraverso le quali circolano i dati. Già LOSANO, voce *Giuscibernetica*, in *Nss. Dig. It. – Appendice (Dis-Impo)*, Torino, 1982, 1077-1098, in part. 1081-1092, descriveva analiticamente i rapporti fra informatica giuridica, logica formale, *hardware* e *software* chiarendo l'importanza dell'elaborazione elettronica quale processo logico di trasformazione di simboli algebrici o elettromeccanici – secondo i modelli disponibili all'epoca – in elaborazioni linguistiche, fondamentali ai fini dell'istituzione di banche dati legislative e giurisprudenziali e, di conseguenza, alla circolazione e al reperimento rapido delle informazioni; inoltre, descriveva analiticamente i modelli reticolari mediante i quali «varie attività vengono concatenate l'una con l'altra in vista del raggiungimento della finalità prefissata», sottolineando l'importanza delle tecniche ad essi collegati ai fini delle procedure giuridiche.
Da tale punto di vista, è rappresentativo il confronto fra due voci del *Digesto delle discipline penalistiche*: MUCCIARELLI, voce *Computer (disciplina giuridica del) nel diritto penale*, in *Dig. Pen., Vol. II C-Conco*, Torino, 1988, 373-390, pone l'attenzione soprattutto sui terminali rappresentati dai singoli elaboratori elettronici e dalla loro rete; PICA G., voce *Internet*, in *Dig. Pen., Agg. II*, Torino, 2004, 427-483, in part. 430 laddove pone l'accento, soprattutto, sulla struttura prevalentemente per *software* e protocolli di Internet, sottolineando così la recessività degli elementi più "materiali" rappresentati dagli *hardware*.
In tempi più recenti, PICA G., *I reati nella società dell'informazione*, in ALEO – PICA, *Diritto penale. Parte Speciale II*, Padova, 2012, 969-1028, in part. 1015-1018, hanno offerto una definizione di Internet quale «sistema di comunicazione globale, basato fisicamente sul collegamento "telematico" fra reti locali di sistemi informativi di tutto il mondo, ovunque situati», sottolineando le sue origini militari (*ARPAnet*) ed il suo passaggio da rete privilegiata per la comunicazione di informazioni di alta qualità, basata sulla *netiquette*, a sistema indiscriminatamente aperto ai cercatori di profitto (*profit-seeker*) che scientemente violano la *netiquette*.

Un sistema di simile dinamicità consente di porre in relazione soggetti ed oggetti distanti fra di loro per qualsiasi scopo: i computer sono diventati uno «strumento del traffico economico» che ha «sostituito la funzione di documentazione della tenuta contabile» e dell'amministrazione[2], utilizzabile peraltro anche per scopi ludico-ricreativi, consumistici e di relazione interpersonale. Tuttavia, il medesimo sistema presenta anche un rovescio della medaglia, rendendo possibile il perseguimento di fini illeciti connessi in modo peculiare allo strumento informatico[3].

Quest'ultimo può rappresentare, da un lato, un *mezzo* di esecuzione privilegiato, parlandosi in tal caso reati informatici in senso lato o *computer crimes*: così avviene, ad esempio, nelle truffe commesse con il ricorso al mezzo informatico, rispetto alle quali la comunicazione a distanza riesce particolarmente efficace quale modo per indurre nella vittima una falsa rappresentazione della realtà[4]. Altri esempi di rilievo possono essere rinvenuti anche nella propaganda di idee a cui i singoli ordinamenti possono attribuire rilievo penale[5], o nell'abuso dei mezzi di pagamento[6], o ancora nel *cyber*-terrorismo[7], o infine nel recentemente introdotto reato di diffusione illecita di immagini o video sessualmente espliciti (art. 612-*ter* cod. pen.)[8].

---

[2] In questi termini TIEDEMANN, *Wirtschafisstrafrecht. Besonderer Teil*, München, III ed. 2011, 285.

[3] Sempre LOSANO, *op. cit.*, pp. 1092-1096, pone l'accento sull'elemento, allora del tutto innovativo, del flusso transnazionale di dati e dei "pericoli" per l'individuo, intesi non necessariamente in un'accezione negativa, connessi a tale traffico. Il principale pericolo è rappresentato dalla possibilità di raccogliere dati che il singolo non vorrebbe fornire: procedura che può essere utilizzata sia a fini investigativi (si fa l'esempio dell'arresto del terrorista Rolf Heissler) sia a fini criminali e di traffico di dati.

[4] Cfr., in argomento, la recentissima pronuncia Cass., Sez. II Pen., Sentenza 6 settembre 2018, n. 40045, in tema di truffa tramite il mezzo informatico. Il soggetto attivo induceva le vittime a disporre trasferimenti di denaro su una carta prepagata dopo averli indotti in errore offrendo loro oggetti in vendita su internet e prestando garanzie, grazie al medesimo strumento, sulla propria affidabilità di venditore.

[5] Sul punto, sul quale si tornerà *infra*, cfr. SATZGER, *Internationales und Europäisches Strafrecht*, Baden-Baden, 2011, 61-66, e GILLESPIE, *Cybercrime. Key Issues And Debates*, New York, 2016, 1-21 – a proposito di quest'ultima opera cfr. la recensione di SALVADORI, pubblicata su *archiviodpc.dirittopenaleuomo.org* in data 11 maggio 2017, vista il 26 giugno 2020.

[6] Cfr. FLOR, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Rivista italiana di diritto e procedura penale*, 2-3/2007, 899-946, in part. 899 ss.

[7] Cfr. FLOR, *Cyber-terrorismo e diritto penale in Italia*, in FORNASARI, WENIN (a cura di), *Diritto penale e modernità. Nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, Napoli, 2017, p. 354, che afferma la natura "ibrida" del fenomeno del *cyber*-terrorismo.

[8] In argomento, CALETTI, *'Revenge porn' e tutela penale. Prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze angloamericane*, in *Diritto penale contemporaneo – Rivista trimestrale*, 3/2018, 63-100. A p. 66 sottolinea il fondamentale ruolo dell'informatica nella circolazione di immagini a fini di cd. *revenge porn*. A p. 82, inoltre, sottolinea come *cyber crimes* quale l'accesso abusivo ad un sistema informatico possano agevolmente concorrere, in connessione di scopi, con l'appropriazione e la diffusione non consensuale di immagini private.

In alternativa, lo strumento informatico può rappresentare il *fine* delle condotte illecite, laddove l'obiettivo criminale sia l'alterazione di sistemi informatici o l'abuso dei dati contenuti in un *database*, nel qual caso si parla di reati informatici in senso proprio o *cyber crimes*[9].

In entrambi i casi, la possibilità di operare da remoto consente agli autori delle condotte illecite di aggirare le sempre più fragili difese su cui possono contare gli Stati nazionali, agendo così potenzialmente su una dimensione planetaria[10]. In un simile contesto, determinare il *locus commissi delicti*, ove per i

---

[9] Le distinzioni cui qui si fa riferimento sono riprese da AMATO, DESTITO, DEZZANI, SANTORIELLO, *Il diritto penale delle nuove tecnologie*, Padova, 2007, 55-56; SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale,* Milano, 2010, il quale alle pp. 7-24 enumera e definisce quelli che ritiene i «settori critici della società informatizzata» e offre una sua definizione delle categorie di reati informatici alle pp. 61-65; NERI, *Criminologia e reati informatici. Profili di diritto penale dell'economia*, Napoli, 2014, in particolare il capitolo di apertura *Cyber crimes: l'approccio criminologico* di cui alle pp. 1 ss.; CHAWKI, *L'individu face à la cybercriminalité*, in CÉRÉ, RASCAGNÈRES, VERGÈS, *Droit penal et nouvelles technologies*, Paris, 2015, 35-57, in part. 37-39 laddove critica come imprecise e poco definitive le definizioni di cybercriminalità date da circolari ufficiali del Ministero dell'Interno della Repubblica francese e dalla Polizia Federale della Confederazione Elvetica, puntualizzando quindi come oggetto di questi crimini «*au moyen d'un systeme d'information et de communication, principalment internet*».

[10] Cfr. PICA G., *I reati nella società dell'informazione*, cit., 969-978, il quale offre un'interessante panoramica sugli studi filosofici, sociologici e giuridici pubblicati a partire dal secondo dopoguerra. Si cita *in primis* WIENER, *Cybernetics, or control and communication in the animal and the machine*, Cambridge (Massachussets), 1948, il cui studio è noto per aver paragonato il funzionamento dei primi sistemi di elaboratori elettronici a quello del sistema nervoso umano in quanto reti di trasmissioni di impulsi.

Con riguardo a quelli pubblicati da metà anni '60 in poi ricordiamo innanzitutto MCLUHAN, *Understanding Media: The Extensions of Man*, New York City, 1964, il quale riprende e sviluppa la metafora del Wiener ed è fra i primi a parlare di «*villaggio globale*». Va precisato che egli ricolleghi a tale espressione un significato profondamente negativo, dal momento che il villaggio, diversamente dalla città, non avrebbe una struttura che porti alla concordia e alla comunicazione fra vicini, bensì piuttosto favorirebbe la chiusura in sé stessi e il sospetto: «*The tribal-global village is far more divisive - full of fighting - than any nationalism ever was. Village is fission, not fusion, in depth.* (...) *The village is not the place to find ideal peace and harmony. Exact opposite.*» (p. 175). Un simile assunto si presta particolarmente bene, da un punto di vista filosofico, a spiegare anche alcune delle possibili cause della criminalità informatica. A commento di tale opera cfr. SING-NAN FEN, *Marshall McLuhan's "Understanding Media"*, in *The Journal of Educational Thought (JET)-Revue de la Pensée Éducative*, 3/1969, 161-180.

Una menzione speciale è dovuta al celebre rapporto alla Presidenza della Repubblica francese sul tema dell'informatizzazione della società: NORA-MINC, *L'informatisation de la société*, Paris, 1978.

In sede comunitaria è d'obbligo menzionare DELORS, *Libro bianco della Commissione per il Consiglio europeo (Milano, 28-29 giugno 1985) COM(85) 310*, 1985, che sottolinea la democratizzazione dell'accesso alle informazioni mediante l'informatica – in materia di impatto dell'informatica sulla società.

PICA G., *ibidem*, adottando la specifica ottica dello studioso di diritto penale, sottolinea quanto l'informatica abbia trasformato la società industriale in una società dell'informazione. In tal guisa giustifica la scelta di collocare, nella sistematica dell'opera manualistica da ALEO-PICA, *op. cit.*, i comunemente detti reati informatici nella trattazione dei "reati della società dell'informazione". Con particolare riguardo alla circolazione globale dei dati lungo le reti elettroniche, il suddetto Autore parla di una dilatazione dei processi digitalizzati «*nello spazio e nel tempo, (...) eliminando le barriere politiche e nazio-*

reati comuni vigono, *in primis*, il principio di territorialità "temperato" e, secondariamente, quello di personalità attiva o passiva, può diventare particolarmente arduo.

Infatti, in uno scenario così configurato, le componenti del primo elemento della scomposizione analitica del reato, vale a dire la tipicità del fatto – condotta, evento, nesso causale – trovano il loro reale punto d'incontro in un siffatto non-luogo. A ciò s'aggiunge la complessità consistente nell'indagare su tali condotte, nel fissare il luogo dell'evento e nel determinare, in tal maniera, la legge applicabile.

L'intervento dei legislatori e delle magistrature, considerata la frequente asistematicità degli atti legislativi preposti all'introduzione dei reati informatici e i contrasti che talora insorgono fra differenti ordinamenti nazionali – talora, pur se inseriti nell'ambito di contesti sovranazionali che dovrebbero favorire l'uniformità delle legislazioni, come l'Unione Europea – appare spesso tardivo ed inefficace[11].

Tuttavia, è evidente che da esso non si possa prescindere. Considerata l'assenza di un governo centrale o di un'autorità regolatrice nel contesto di *Internet*, le istanze che spingano gli utenti della rete ad autoregolarsi tramite la *netiquette* o altri protocolli per lo più di natura etica, pur se dotati di appigli testuali che fanno ricorso a linguaggio e concetti tipicamente giuridici[12], non possono che essere destinate al fallimento. Rimane quindi un compito essen-

---

nali, che nella dimensione analogica bloccavano e controllavano l'interscambio informativo e la comunicazione».

In tempi recenti, il problema della transnazionalità del reato informatico è stato posto in particolare evidenza dalla conferenza dello *International Scientific and Professional Advisory Council of the United Nations (ISPAC)* tenutasi a Courmayer dal 2 al 4 dicembre 2011, disponibili presso *http://ispac.cnpds.org/report-international-conference-on-cybercrime-global-phenomenon-and-its-challenges-32.html* (visto da ultimo il 26 giugno 2020). Cfr. il report di PISAPIA, *Le sfide globali dei 'cybercrimes'*, in *archiviodpc.dirittopenaleuomo.org*, pubblicato il 10 dicembre 2011, visto il 26 giugno 2020.

[11] Cfr. PICA G., *I reati nella società dell'informazione*, cit., pp. 1018 ss.

[12] È il caso, *inter alia*, della *Internet Magna Charta* proposta da Tim Berners Lee, nonché della *Declaration of Internet Rights* formulata dalla *Commissione di studio per l'elaborazione di principi in tema di diritti e doveri relativi ad Internet* istituita dal Parlamento della Repubblica italiana, pubblicata il 28 luglio 2015. Fra gli Autori dottrinali fautori di una soluzione "costituzionale" per il governo della rete, si segnala RODOTÀ, *Il mondo della rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, in part. 61 ss. Le proposte che vadano nel senso di proporre una carta costituzionale del *web*, a modesto avviso di chi scrive, sono basate su un equivoco di fondo: quello in base al quale la rete possa essere governata al pari di uno Stato, o anche di un organismo sovranazionale. A ben vedere, la rete non presenta nessuno dei caratteri fondamentali di un'entità statale o sovrastatale: non quelli della giuspubblicistica tradizionale, dal momento che *Internet* non ha un territorio, non ha un popolo, né tantomeno può esserne centralizzata l'amministrazione, vieppiù che una "rete" è concepita, peraltro, per non avere un centro; né quelli della giuspubblicistica più moderna, che si esprime in termini di monopolio della forza.

ziale delle compagini statali e sovra-statali il contrasto ad una criminalità che, pur muovendosi in un non-luogo smaterializzato, presenta degli effetti talora molto concreti nella vita dei singoli e delle collettività[13], nel contesto di un sistema socio-economico improntato alla circolazione di informazioni e di contatti personali a distanza che non è più in grado di fare a meno dell'informazione digitale[14].

In relazione ad alcune categorie di reati, la soluzione risulta più agevole attraverso l'individuazione di una vittima ai danni della quale si possa ritenere verificato l'evento del reato o di un potenziale interessato da condotte concretamente pericolose: ciò consente, sul piano sostanziale, di identificare il luogo di commissione del reato e, ai fini processuali, di radicare la competenza territoriale. Ben più complessa è la risoluzione di quei casi in cui la vittima del reato non sia identificabile in una data persona fisica, concernendo il danno o – ancor peggio – il pericolo una pluralità di soggetti non identificabili *a priori* o la "pubblica utilità". Il presente contributo intende focalizzarsi su questa seconda categoria di fattispecie.

2. Locus commissi delicti *ed evento nei reati informatici. Norme di collegamento: una panoramica sul diritto italiano e gli ordinamenti stranieri*. Il riferimento agli elementi che compongono la struttura del fatto tipico è, infatti, un criterio essenziale sia per la "collocazione" del fatto di reato e, conseguentemente, per l'individuazione della legge applicabile, sia, in termini processuali, per la determinazione della giurisdizione competente.

I principali modelli ipotizzabili per il collegamento tra fatto di reato e normativa applicabile, nel contesto di un principio di territorialità, come è noto, sono il criterio della condotta, quello dell'evento e il criterio dell'ubiquità, sintetizzabili nei termini che seguono[15].

---

[13] Cfr. SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, cit., che alle 73-77 enumera le dimensioni e i costi dei reati informatici a partire da metà anni '70 fino a metà del decennio scorso; CHAWKI, *L'individu face à la cybercriminalité*, 39-41, il quale rimanda ai dati raccolti dall'associazione CLUSIF - *Club de la Sécurité de l'Information Français* - e ripresentati annualmente in una conferenza, *https://clusif.fr/*.

[14] In termini non dissimili, più diffusamente, PICA G., voce *Internet*, 427-429 e 481-483. Lo stesso Autore muove il rilievo sull'irrinunciabilità dell'utilizzo della tecnologia dell'informazione digitale al fine di porre in evidenza l'ambivalenza della stessa ai fini del diritto penale in PICA G., *I reati nella società dell'informazione*, cit., 978-979.

[15] In argomento, per una ricognizione sintetica ma completa, cfr. i manuali istituzionali di ANTOLISEI, CONTI, *Manuale di diritto penale. Parte generale*, Milano, XVI ed. 2003, 119-121; FIANDACA, MUSCO, *Diritto penale. Parte generale*, Bologna, VII edizione 2014, 139 ss.; MANTOVANI, *Diritto penale. Parte generale*, Padova, IX ed. 2015, 878 ss.; FIORE C., FIORE S., *Diritto penale. Parte generale*, Torino, 2016, 118 ss.; ROMANO B., *Diritto penale. Parte generale*, Milano, 2016, 175 ss. Per quanto riguarda il diritto tedesco, cfr. WESSELS, BEULKE, SATZGER, *Strafrecht Allgemeiner Teil. Die Straftat und ihr Auf-*

Il criterio della condotta, solitamente improntato ad un diritto penale di matrice soggettivistica, fissa il *locus commissi delicti* nel luogo in cui il soggetto attivo ha commesso il fatto ovvero quello nel quale si sarebbe dovuto attivare per evitare il verificarsi dell'evento.
Il criterio dell'evento, improntato ad un diritto penale di matrice oggettivistica, fissa il *locus commissi delicti* nel luogo in cui si verifica la modificazione della realtà esteriore – secondo la cd. concezione naturalistica dell'evento – conseguente alla condotta.
Il criterio dell'ubiquità assomma i due criteri precedenti attribuendo rilevanza alternativa o congiunta ad entrambi gli elementi, in modo da conferire la massima attrattività alla legge penale di riferimento, ed è tipico di una concezione mista del diritto penale. Tale è quello seguito nella maggioranza degli ordinamenti eurocontinentali, per esempio dai Codici penali italiano (art. 6) e francese (art. 113-2)[16], nonché dagli *Strafgesetzbuch* tedesco (§ 9)[17] ed austriaco (§ 67 comma 2)[18].

---

bau, Heidelberg, 44ma ed. 2014, 23 ss.; RENGIER, *Strafrecht Allgemeiner Teil*, München, XI ed. 2019, 33 ss.
Per un'analisi più approfondita, VINCIGUERRA, *Diritto penale italiano. Vol. I: Concetto, fonti, validità, interpretazione*, Padova, II edizione 2009, 360 ss.; SATZGER, *StR Das deutsche Strafanwendungsrecht (§§ 3 ff. StGB) – Teil 1*, in *Juristische Ausbildung*, 2/2010, 112 ss.; ID., *Internationales und Europäisches Strafrecht*, cit., pp. 44 ss.; TIEDEMANN, *Wirtschaftsstrafrecht. Einführung und Allgemeiner Teil*, München, IV ed. 2014, 171 ss.
Per un focus più specifico sui reati informatici, GILLESPIE, *Cybercrime*, cit., 21 ss.; SATZGER, *ibidem* (v. *infra*, note seguenti).

[16] Testo originale della disposizione: «*La loi pénale française est applicable aux infractions commises sur le territoire de la République. L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire*».

[17] Testo originale della disposizione, comma I: »*Eine Tat ist an jedem Ort begangen, an dem der Täter gehandelt hat oder im Falle des Unterlassens hätte handeln müssen oder an dem der zum Tatbestand gehörende Erfolg eingetreten ist oder nach der Vorstellung des Täters eintreten sollte*«. Traduzione, a cura dello scrivente: «Un fatto è commesso nel luogo nel quale il soggetto attivo ha agito o, in caso di un'omissione, avrebbe dovuto agire, o nel quale l'evento del fatto tipico si sia verificato o si sarebbe dovuto verificare secondo la rappresentazione del soggetto attivo».
Il comma II del medesimo paragrafo, che riproduce il linguaggio concettuale del I, riguarda il fatto tipico di concorso di persone (*Teilnahme*), prevedendo che esso si collochi sia nel luogo dove si è verificato il fatto principale (*Tat*), sia in quello dove il concorrente abbia agito, avrebbe dovuto agire o in quello nel quale, secondo la sua rappresentazione, il fatto si sarebbe dovuto verificare. Nel caso in cui il fatto del concorrente sia commesso all'estero, anche ad esso si applica il diritto tedesco, anche se secondo la *lex loci* non costituisca reato. Anche il fatto del concorrente è quindi attratto nella sfera di applicazione del diritto tedesco.
A tal proposito, è bene ricordare che lo *Strafgesetzbuch* tedesco adotta un modello differenziato per il concorso di persone (§§ 25 ss. *StGB*): sul tema, in lingua italiana, in ottica (anche) comparatistica, MANTOVANI, *Diritto penale. Parte generale*, cit., 505 ss.; HELFER, *Il concorso di più persone nel reato. Problemi aperti del sistema unitario italiano*, Torino, 2013, in part. 10 ss., 274 ss.

[18] Testo originale della disposizione: »*Eine mit Strafe bedrohte Handlung hat der Täter an jedem Ort*

In relazione ai reati informatici, il ricorso ad una "fisicizzazione" degli elementi del fatto tipico, collocando la condotta nel luogo in cui si trova il soggetto attivo e l'evento in quello in cui si trova il soggetto passivo, può apparire in determinati casi risolutivo. Una siffatta operazione non ha affatto un carattere fittizio, dal momento che opera l'unico possibile collegamento reale fra i protagonisti del reato informatico e il mondo fisico, conferendo così dimensione materiale al fatto.

Al riguardo, è degna di nota la soluzione adottata in seno all'ordinamento francese: l'art. 113-2-1 del *Code pénal*, introdotto nel 2016, ha infatti sancito la fissazione nel proprio territorio nazionale del *locus commissi delicti* dei reati commessi «per mezzo di una rete di comunicazione elettronica» qualora il reato sia stato commesso o tentato ai danni «di una persona fisica residente nel territorio della Repubblica o di una persona giuridica la cui sede sia situata nel territorio della Repubblica»[19].

Tuttavia, i modelli qui rappresentati diventano particolarmente ardui da applicare quando il reato commesso dal soggetto attivo *non abbia* un soggetto passivo determinato o determinabile e la condotta si sia svolta all'estero, rendendo così difficile la collocazione dell'evento. Questo è il caso dei reati a soggetto passivo indeterminato.

3. *Il problema dei reati informatici a soggetto passivo indeterminato.* Sotto la definizione di reati a soggetto passivo indeterminato – detti anche reati vaghi o vaganti – si riconducono, di norma, quelle figure caratterizzate dall'assenza di un portatore degli interessi lesi dal reato individuato o individuabile tramite il disposto della norma[20]. Tale categoria di illeciti penali assolve, dunque, ad una funzione di tutela di interessi non riconducibili ad entità soggettive de-

---

begangen, an dem er gehandelt hat oder hätte handeln sollen oder ein dem Tatbild entsprechender Erfolg ganz oder zum Teil eingetreten ist oder nach der Vorstellung des Täters hätte eintreten sollen». Traduzione, a cura dello scrivente: «Una condotta minacciata da pena è commessa dal soggetto attivo nel luogo nel quale egli ha agito o avrebbe dovuto agire o nel quale si sia verificato, interamente o in parte, un evento corrispondente a quello della descrizione del fatto, o vi si sarebbe dovuto verificare secondo la rappresentazione del soggetto attivo».

[19] Testo originale della disposizione: «*Tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République*».

Soluzioni non distanti da questa vengono adottate dalla giurisprudenza di legittimità italiana per definire la competenza dei tribunali e delle corti territoriali: cfr. a tal proposito Cass., Sez. III Pen., Sentenza 27 settembre 2013, n. 40403.

[20] Per una prima, sintetica definizione del fenomeno cfr. di ANTOLISEI, CONTI, *Manuale di diritto penale. Parte generale*, cit., 187-191; MANTOVANI, *Diritto penale. Parte generale*, cit., 225-234; di FIORE C., FIORE S., *Diritto penale. Parte generale*, cit., 184-186.

terminate, individuali o collettive, essendo i potenziali interessati un insieme potenzialmente aperto e privo di confini.
L'anticipazione della tutela richiede di essere giustificata, in termini di politica criminale, tramite le peculiarità che connotano i beni giuridici protetti, rendendo utili, se non necessarie, forme di prevenzione del danno a suddetti beni. Una loro definitiva compromissione, infatti, potrebbe avere riflessi molto gravi in termini di importanza del bene giuridico o di vittimizzazione di massa[21].
Conviene, pertanto, dedicare una sintetica analisi al tema dei beni oggetto di protezione tramite l'istituzione di figure di reato a soggetto passivo indeterminato e all'eventuale sussunzione di *Internet* e dei beni ad esso correlati nelle categorie che verranno così circoscritte.
3.1. *Beni a titolarità diffusa, beni pubblici, beni collettivi. La natura di* Internet. I beni giuridici la cui tutela si persegue, mutuando il linguaggio della scienza economica, possono essere sostanzialmente indicati nei beni a titolarità diffusa, siano essi da categorizzarsi ulteriormente come beni pubblici o come beni collettivi *stricto sensu*.
La titolarità diffusa di un bene comporta che esso, in relazione al suo utilizzo da parte di uno o più operatori privati[22], (i) non sia rivale: vale a dire, che sud-

[21] Lo stato attuale della discussione sul bene giuridico protetto è descritto nel migliore dei modi, ad avviso di chi scrive, soprattutto da FIANDACA –MUSCO, *Diritto penale. Parte generale*, cit., XIII-XXXVII e 3 ss. Si segnalano inoltre le trattazioni di DE VERO, *Corso di diritto penale*, Torino, II ed. 2012, pp. 118 ss.; MANTOVANI, *Diritto penale. Parte generale*, cit., 194 ss.; FIORE C., FIORE S., *Diritto penale. Parte generale*, cit., 5 ss., 179 ss.; PALAZZO, *Corso di diritto penale. Parte generale*, Torino, VII ed. 2018, 62 ss.; CADOPPI –VENEZIANI, *Elementi di diritto penale. Parte generale*, Padova, VII ed. 2018, 103-118.
Nella manualistica tedesca, autorevole e approfondita è la trattazione da parte di ROXIN, *Strafrecht Allgemeiner Teil*, Vol. I – *Grundlagen. Der Aufbau der Verbrechenslehre*, München, IV ed. 2006, pp. 8-63. Più sintetici sono GROPP, *Strafrecht Allgemeiner Teil*, Berlin-Heidelberg, IV ed. 2015, pp. 37-39; WESSELS, BEULKE, SATZGER, *Strafrecht Allgemeiner Teil*, cit., 3-5, *passim*.
Per quanto riguarda gli scritti storici sul tema, si aderisce alla visione formulata soprattutto da alcuni Autori tedeschi del diciannovesimo secolo: in particolare, quella liberale-tardoilluministica di BIRNBAUM, *Ueber das Erfordernis einer Rechtsverlezung zum Begriffe des Verbrechens*, in *Archiv des Criminalrechts*, 1834, 149-195 – di cui segnalo la mia traduzione in lingua italiana: *Sulla necessità della violazione di un diritto per il concetto di reato*, in *Diritto penale XXI Secolo*, 1/2019, 115-142, a cura di CAMPLANI – e quella positivistico-naturalistica di VON LISZT, *Rechtsgut und Handlungsbegriff im Bindingschen Handbuche. Ein kritischer Beitrag zur juristischen Methodenlehre*, in *ZStW*, 1886 (Vol. 6), 663-698, e in ID., *Der Begriff des Rechtsgutes im Strafrecht und in der Encykolpädie der Rechtswissenschaft*, in *ZStW*, 1888 (Vol. 8), 133-156. Fra gli Autori italiani si fa riferimento soprattutto a BRICOLA, voce *Teoria generale del reato*, in *Nss. D.I.*, Vol. XIV, Torino, 1973, pp. 7-93, con riferimento alla costituzionalizzazione del bene giuridico.
[22] L'analisi più approfondita in materia, cui si rimanda, è quella di DE VITA, *I reati a soggetto passivo indeterminato. Oggetto dell'offesa e tutela processuale*, Napoli 1999. Il tema dei beni giuridici protetti dai reati a soggetto passivo indeterminato e del loro legame concettuale con i beni studiati dalle scienze

detto uso da parte di uno o più operatori non osti al suo utilizzo da parte di altri; (ii) non sia escludibile: in altri termini, che eventuali azioni volte a limitarne l'uso siano in concreto impossibile.
In tal misura, un siffatto bene assolve ad interessi diffusi, non prestandosi alla titolarizzazione di uno o più appartenenti ad una comunità nazionale[23] o anche – come appare sempre più evidente, alla luce dei recenti sviluppi delle relazioni fra Stati e cittadini – internazionale o transnazionale. In tal misura, esso rappresenta una ipotesi in cui il mercato fallisce, non potendo raggiungere un'allocazione equa, socialmente efficiente o equilibrata di simili beni. Rispetto ad essi, le attività private possono rappresentare esternalità positive o negative, dal momento che possono rappresentare un vantaggio o un costo ai fini della loro fruizione[24].
Internet, ad oggi, presenta in buona sostanza tutti i requisiti di un bene a titolarità diffusa. Il suo utilizzo da parte di un certo numero di utenti non impedisce, in concreto, quello da parte di altri. Le possibili restrizioni al suo utilizzo poste dall'intervento pubblico di alcuni Stati, specie quelli retti da un sistema totalitario, sono facilmente aggirabili. L'attività del settore pubblico non risulta decisiva ai fini della sua esistenza – se non per quanto riguarda le origini come rete militare *ARPAnet* – ma potrebbe assumere un ruolo fondamentale ai fini della sua diffusa, democratica e corretta fruizione, quantunque i poteri degli Stati si dimostrino decisamente deboli di fronte ad una rete senza territorio e con una base fisica che ben poco rivela dei contenuti presenti sulla stessa.
Lo stesso non può sempre dirsi dei dati e dei sistemi informatici, rispetto ai quali è possibile porre barriere d'ingresso – sistemi di autenticazione, *password* – e identificare una titolarità ben precisa, se non addirittura la diretta pertinenza ad una personalità fisica[25]. Questo si riflette, immancabilmente, nella distinzione fra reati informatici in cui il soggetto passivo è determinabile da quelli in cui rimane indeterminato.
Le ulteriori categorizzazioni menzionate si rendono utili al fine di distinguere i beni nei quali si registri l'intervento di mercato degli operatori pubblici.

---

economiche è trattato soprattutto nel Cap. I, 27 ss., e nel Cap. II, dedicato all'analisi dei profili riguardanti il rapporto di detti reati con il principio di offensività, 95 ss.
[23] Cfr. DE VITA, *I reati a soggetto passivo indeterminato*, cit., 27-30.
[24] Cfr., nella letteratura economica, SLOMAN, GARRAT, *Essential of economics*, Harlow, 2010, traduzione italiana a cura di Amighini, Cincotti, Landi, *Microeconomia*, Bologna, 2010, 184 ss.; CAMPA, *Lezioni di scienza delle finanze*, Torino, 2010, 151 ss.
[25] Cfr. PICA G., *I reati nella società dell'informazione*, cit., 979 ss. sui dati personali; 996 ss. sulla natura dei dati quale informazione posta in forma elettronica e sulla natura dei sistemi informatici.

Per beni pubblici, si intendono non tanto e non solo i beni facenti capo alla titolarità dello Stato o di altri enti pubblici, bensì anche quelli che rappresentino «il risultato utile di un'attività svolta in via di principio dal settore pubblico» e che rimangono insuscettibili di una appropriazione *anche* da parte dei privati[26]. I beni pubblici che possano essere riguardati dalla criminalità informatica sono quelli dei sistemi informatici *di pubblica utilità*, alcuni dei quali fanno capo ad enti pubblici, mentre in altri casi si tratta di «*impianti di gestione di servizi per una collettività indifferenziata di persone*»[27].
Quali beni collettivi *stricto sensu* possono essere indicati, invece, quelli, del pari non rivali, non escludibili e quindi insuscettibili di appropriazione esclusiva, che invece ammettano la coesistenza di una titolarità privata. Essa di per sé sarebbe, anzi, l'elemento caratterizzante tali beni; l'interesse collettivo, consistente nelle esternalità positive che la fruizione di tali beni arreca alla generalità, giustifica tuttavia la limitazione della libera disposizione di tale bene da parte dei titolari privati[28].
La sicurezza delle comunicazioni informatiche, della circolazione dei dati e dei sistemi informatici potrebbe essere considerata rientrante in questa seconda categoria. Infatti, se da un lato se ne giova innanzitutto ciascun utente della rete singolarmente considerato, dall'altro ne beneficia collettivamente l'intero pubblico degli utenti. Tanto rende utile che nessun utente accetti di ricorrere a pratiche o misure insicure in cambio di vantaggi di altra natura, come d'altronde evidenzia l'affermazione di figure come i *Data protection officers*.
Entrambe le categorie di beni non consentono, o consentono solo in parte, forme di coincidenza concettuale fra l'offesa di rilevanza pubblica sussunta nella previsione di reato e la dimensione essenzialmente privatistica rappresentata dall'illecito aquiliano, con i conseguenti riflessi in termini processuali[29].

---

[26] Cfr. DE VITA, *I reati a soggetto passivo indeterminato*, cit., 29, laddove cita a sua volta PICA F., *Economia pubblica*, Torino, 1987, p. 133. Quale esempio paradigmatico, l'Autore indica l'ambiente, che evidentemente non è un bene prodotto dal settore pubblico ma la cui tutela è il risultato dell'attività dello stesso. Sui beni pubblici si vedano anche SLOMAN, GARRAT, *op. cit.*, 190 ss.; CAMPA, *Lezioni*, cit., 161 ss.
[27] Così PICA G., *I reati nella società dell'informazione*, cit., 1009.
[28] Cfr. DE VITA, *I reati a soggetto passivo indeterminato*, cit., 33, laddove cita a sua volta TROCKER, *Interessi collettivi e diffusi*, in *Enciclopedia Giuridica Treccani* Roma, 1989, 1. Quale esempio paradigmatico, l'Autore indica la salute, bene di cui evidentemente gode *in primis* l'individuo, quantunque indubbiamente la salute del singolo arrechi beneficio all'intera comunità; analogo esempio, nella trattazione dei reati di pericolo astratto, è proposto da FIORE C., FIORE S., *Diritto penale. Parte generale*, cit., 198. CAMPA, *Lezioni*, cit.,2010, 179, riprendendo la terminologia di MUSGRAVE, *A Multiple Theory Of Budget Determination*, in *Finanz Archiv*, 1957, 33-43, li presenta come "beni di merito" (*merit wants*).
[29] Cfr. DE VITA, *I reati a soggetto passivo indeterminato*, cit., 121 ss.

La tutela di siffatti beni rende utile, di norma, una strategia politico-criminale volta ad anticipare la punibilità tramite fattispecie di pericolo, soprattutto astratto. Le condotte dei reati a soggetto passivo indeterminato sono, infatti, generalmente anticipate ad un momento nel quale non è ancora possibile ravvisare la concreta lesione di un bene giuridico. In relazioni a tali fattispecie, l'evento lesivo del bene giuridico rappresenterebbe un danno irreparabile o comporterebbe una "vittimizzazione di massa": anche per questo, dall'anticipo della punibilità, risulta solitamente un soggetto passivo indeterminato[30]. Nell'ambito dei reati informatici, si pensi al caso della messa in pericolo di sistemi informatici per la difesa nazionale o alla diffusione di tesi revisioniste per mezzo di siti internet: lasciare che *iter* criminosi connessi a simili reati sfocino in un evento delittuoso potrebbe avere conseguenze molto gravi per un numero di persone estremamente ampio, peraltro potenzialmente ben al di là dei confini di una singola nazione.

Seguendo la classificazione tratteggiata nell'introduzione e gli esempi testé richiamati, è possibile rinvenire figure di reato a soggetto passivo indeterminato sia nella categoria dei *cyber crimes* che in quella dei *computer crimes*, tanto nell'ordinamento italiano quanto negli ordinamenti di altri Stati che hanno ratificato la Convenzione di Budapest. Il diritto tedesco, in virtù degli autorevoli studi compiuti in argomento fin dagli anni Novanta e di alcuni arresti giurisprudenziali di grande risonanza in materia, si presenta quale interessante termine di paragone.

3.2. *I reati informatici in senso proprio o cyber crimes. La prospettiva del diritto italiano*. La criminalizzazione di condotte concernenti i sistemi informatici, dopo i primi passi mossi dai singoli ordinamenti statali, ha ricevuto un'impronta più uniforme e sistematica grazie alla Convenzione del Consiglio d'Europa sulla Criminalità Informatica, siglata a Budapest nel 2001 e preceduta da un lavoro quadriennale di esperti europei, nordamericani e giapponesi[31].

Com'è noto, i reati informatici sono stati localizzati, dal legislatore italiano,

[30] Cfr. DE VITA, *op. ult. cit.*, 75 ss. sulla struttura e funzione dei reati a soggetto passivo indeterminato, in part. 90-94 sulla questione dell'anticipazione della tutela penale.

[31] I reati informatici hanno fatto ingresso nel Codice penale italiano grazie alle leggi n. 547 del 1993 e 48 del 2008 – quest'ultima, emanata in recepimento della Convenzione sopra menzionata. In dottrina cfr. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Diritto penale e processo*, 6/2008, 700-716, che commenta la legge di recepimento della convenzione; PICA G., *I reati nella società dell'informazione*, cit., 991 ss.; PECORELLA, *Reati informatici contro il patrimonio*, in PULITANÒ (a cura di), *Diritto penale. Parte speciale – Volume II: I delitti contro il patrimonio* Torino, 2013, 271-293; NERI, *Criminologia e reati informatici*, cit., 47-48.

prevalentemente in due sub-partizioni del Libro II del codice penale, ponendoli in prossimità di fattispecie tradizionali loro più rassomiglianti[32].
Per fornire al quadro complessivo della materia una sistematicità che non si ricava dal testo di legge, è possibile ricorrere una quadripartizione così riassumibile[33]:
quelli diretti contro i dati che circolano tramite le comunicazioni informatiche, sia (a_1) pubbliche che (b_1) private, volti ad intercettare, ad alterare i dati o a farne oggetto di appropriazione e circolazione abusiva – detti anche reati di spionaggio informatico (*Computerspionage*)[34] – sono categorizzati fra i delitti contro la libertà individuale, più nello specifico fra quelli contro l'inviolabilità del domicilio;
quelli diretti a danneggiare i sistemi informatici, sia di (a_2) pubblica che di (b_2) privata utilità, volti a rendere inservibili (almeno temporaneamente) i dati senza alterarne la sostanza – detti anche reati di sabotaggio informatico (*Computersabotage*)[35] – sono interpolati fra i delitti contro il patrimonio e ricevono un trattamento sanzionatorio di maggior rigore.
Alcune di queste figure delittuose, quali quelle degli artt. 615-*ter*[36], 635-*bis* e 640-*ter* cod. pen., sono state configurate come reati di evento. Tanto consente di determinare agevolmente un soggetto passivo, privato o pubblico, nel titolare dei dati o del sistema informatico.
Tuttavia, ampio ricorso si è fatto a reati di condotta improntati secondo lo schema del pericolo concreto o astratto: in tali altre fattispecie, il titolare dei

[32] Cfr. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004, 42-47, il quale giudica positivamente la scelta di collocare i reati informatici nel codice penale e di seguire la classificazione tradizionale dei beni giuridici; PECORELLA, voce *Reati informatici*, in *Enc. Dir., Annali X*, Milano, 2017, 707-725, in part. 712, laddove ritiene la scelta del legislatore «*del tutto condivisibile*».

[33] Lo schema della quadripartizione è stato proposto, *in primis*, da MANTOVANI *Diritto penale. Parte Speciale. II – I delitti contro il patrimonio*, Padova, IV ed. 2012, 136 ss., e ripreso da MEZZETTI, *Reati contro il patrimonio*, in GROSSO, PADOVANI, PAGLIARO, *Trattato di Diritto penale*, Milano, 2013, 347 ss.

[34] Cfr. PECORELLA, *Diritto penale dell'informatica*, Milano, 2006, 253 ss.: l'Autrice, in quel momento, si richiamava soprattutto alle elaborazioni della dottrina tedesca in materia, in particolare a SIEBER, *Gefahr und Abwehr der Computerkriminalität*, in *BetriebsBerater*, 1982, 1433-1442, in part. 1435.

[35] Cfr. PECORELLA, *Diritto penale dell'informatica*, cit., 233 ss.: anche qui l'Autrice si richiama alla dottrina tedesca – si veda, per tutti, TIEDEMANN, *Computerkriminalität und Strafrecht*, Köln, 1980, 87 ss. – e definisce "logico" questo tipo di illecito, dal momento che aggredisce quella che è la capacità logica del sistema informatico, rendendolo così incapace di funzionare.

[36] In argomento, FLOR, *Permanenza non autorizzata in un sistema informatico o telematico, violazione del segreto d'ufficio e concorso nel reato da parte dell'*extraneus, in *Cassazione penale*, 4/2009, 1509-1525.

dati o del sistema minacciati, in misura più o meno diretta, dalle condotte del soggetto attivo diventa sicuramente più arduo da individuare.

(1) Procedendo in base alla sistematica della quadripartizione poc'anzi menzionata, un primo esempio paradigmatico è rappresentato dall'art. 615-*quinquies* cod. pen., rubricato "Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico".

Tale fattispecie, improntata alla tutela dei sistemi informatici, ovvero dei dati e delle informazioni in essi contenuti, presenta una evidente anticipazione del momento della consumazione del reato. Infatti, le numerose condotte indicate come rilevanti – sufficienti a perfezionare il reato[37] – presentano come caratteristica comune la diffusione, a vario titolo, del mezzo a cui si ricorrerebbe per cagionare tali danni, ovvero «apparecchiature, dispositivi o programmi informatici» che siano astrattamente idonei allo scopo. Non si richiede che né il danno né il relativo pericolo si prospettino in concreto[38].

La dannosità della condotta, a ben vedere, non esula del tutto dalla fattispecie, ma si caratterizza quale mero oggetto del dolo specifico («*allo scopo di danneggiare illecitamente un sistema informatico o telematico*»), vale a dire quale «contenuto della finalità soggettiva dell'agente». Un simile elemento contravviene in sostanza alle direttive della Convenzione di Budapest e revoca in dubbio l'effettivo rispetto del principio di offensività – il che consente di dubitare della legittimità costituzionale della norma[39].

---

[37] MAIORANO, *Sub* Art. 615-*quinquies*, in LATTANZI, LUPO (a cura di), *Codice Penale. Rassegna di giurisprudenza e di dottrina, Vol. VII- I delitti contro la persona* Milano, 2016, 995-999, in part. 999.

[38] Cfr. AMATO, DESTITO, DEZZANI, SANTORIELLO, *Il diritto penale delle nuove tecnologie*, cit., 94 e 117; NERI, *Criminologia e reati informatici*, cit., 77 ss., collocano senza esitazione tali fattispecie nell'ambito dei reati di pericolo, dopo aver preso posizione – ad avviso di chi scrive, condivisibilmente – per la natura di reato di danno in relazione all'art. 615-ter cod. pen. GATTA, *I delitti contro l'inviolabilità del domicilio*, in VIGANÒ, PIERGALLINI, *Reati contro la persona e contro il patrimonio*, in PALAZZO, PALIERO, *Trattato teorico-pratico di diritto penale*, Torino, 2015, 317-359, in part. 357-358, sottolinea le critiche mosse alla collocazione nell'ambito dei delitti contro l'inviolabilità del domicilio informatico e annota lo scarso riscontro della fattispecie in sede giurisprudenziale.

[39] Cfr. PICOTTI, *La ratifica*, cit., 709-710, il quale, dopo aver posto in rilievo la totale mancanza di incidenza oggettiva dell'illiceità delle condotte, che di per sé potrebbero anzi essere perfettamente lecite, afferma che «*La nuova formulazione dell'art. 615-quinquies c.p. è dunque andata nella direzione diametralmente opposta a quella tracciata dalla Convenzione, che richiederebbe di arricchire la qualificazione oggettiva di antigiuridicità speciale del fatto, in conformità con la clausola generale "senza diritto" che compare in questa come in tutte le altre previsioni incriminatrici da essa previste*». Sulla medesima linea, MAIORANO, *Sub* Art. 615-*quinquies*, cit., 997; MINO, *La tutela penale del domicilio informatico*, in ROMANO B. (a cura di), *Reati contro la persona*, in GROSSO, PADOVANI, PAGLIARO, *Trattato di Diritto penale*, Milano, 2016, 487-505, in part. 501-502. Duramente critico riguardo alla descrizione delle condotte, ma decisamente favorevole al correttivo rappresentato dal dolo specifico è PICA G., *I reati*

Il fatto tipico che ne risulta è caratterizzato da una manifesta mancanza di un qualsivoglia evento e da una situazione di pericolo ancora molto lontana financo dalla possibilità di tradurre in concreto la minaccia al bene giuridico protetto. Non appare quindi possibile identificare un soggetto passivo del reato.

L'anticipazione della soglia di rilevanza penale, nel contesto della fattispecie testé richiamata, oltre a rendere non configurabile il tentativo, è quindi talmente accentuata da aver consentito l'inserimento di un'ulteriore fattispecie di pericolo, questa volta concreto, volta a punire l'installazione dei suddetti mezzi (art. 617-*quinquies* cod. pen.)[40].

(2) Fra i reati contro il patrimonio, si possono individuare almeno due figure delittuose che presentino la peculiare struttura oggetto della nostra analisi. Entrambe sono state inserite con la legge 18 marzo 2008 n. 48, emanata in esecuzione della Convenzione di Budapest.

La prima delle due è quella ai sensi dell'art. 635-*ter* cod. pen., rubricata "danneggiamento di dati informatici di pubblica utilità". Essa è collocata a seguito dell'art. 635-*bis* cod. pen., la quale è una fattispecie speciale di danneggiamento avente, quale elemento di specializzazione, l'oggetto del reato, rappresentato appunto da un sistema informatico e dai dati in esso contenuti.

La fattispecie di cui all'art. 635-*ter* comma 1, tuttavia, tradisce in sostanza il suggerimento recato dalla rubrica: essa si caratterizza, innanzitutto, per l'anticipazione della tutela ad un fatto "*diretto*" al danneggiamento di suddetto sistema; in secondo luogo, è possibile osservare che lo Stato o l'ente pubblico indicati quali gestori dei dati non sono necessariamente i titolari dei dati stessi,

---

nella società dell'informazione, cit., 1010-1012. Rileva un arretramento rispetto alla norma previgente, introdotta dalla l. 547/1993, PECORELLA, voce *Reati informatici*, cit., 720-721, laddove sottolinea come essa – pur non esente da criticità – richiedesse un effettivo potenziale dannoso dei dispositivi; confida in «*un'interpretazione della norma che, nel rispetto del principio di offensività, la renda applicabile solo nei casi in cui lo scopo perseguito dall'agente, con una di quelle condotte ancora così lontane dall'offesa, trovi riscontro nella loro oggettiva idoneità a danneggiare i beni informatici altrui*».

Meno critici sembrano FIANDACA-MUSCO, *Diritto penale. Parte speciale – Volume II, tomo primo: I delitti contro la persona*, Bologna, 2013, 298-300, che sottolineano l'importanza che tale norma può avere nel prevenire la circolazione dei virus informatici e nel tutelare il *know-how* connesso ai dati e ai sistemi informatici, evidenziando peraltro quanto una disposizione siffatta consenta di cogliere «*con palmare evidenza*» la funzione selettiva del dolo specifico. Analoga la posizione di PECORELLA, *Reati informatici contro il patrimonio*, cit., 291-293.

[40] Cfr. NERI, *Criminologia e reati informatici*, cit., 77 ss.; AMATO, DESTITO, DEZZANI, SANTORIELLO, *Il diritto penale delle nuove tecnologie*, cit., 94 e 117; GARGIULO, *Sub* Art. 617-*quinquies*, in LATTANZI, LUPO (a cura di), *Codice Penale. Rassegna di giurisprudenza e di dottrina, Vol. VII- I delitti contro la persona*, cit., 1092-1093.

bensì possono essere anche i gestori di dati altrui a fini di "*pubblica utilità*"[41].
L'elemento concretamente dannoso è contemplato dall'autonoma fattispecie di cui al comma 2, che di conseguenza assume la peculiare struttura di reato aggravato dall'evento[42].
Uno schema analogo regola i rapporti con l'altra fattispecie che qui si assume a paradigma, quella dell'art. 635-*quinquies* cod. pen., rubricato "danneggiamento di sistemi informatici di pubblica utilità", con quella che la precede, art. 635-*quater*, rubricato "danneggiamento di sistemi informatici di privata utilità". Anche nel contesto di tale disposizione, si può osservare un primo comma dedicato a condotte, dettagliatamente tipizzate, "*dirette*" a cagionare un danno ad un sistema il cui titolare non sia necessariamente uno Stato o ente pubblico, ma esprima una utilità per un numero potenzialmente ampio ed indeterminato di persone. Il comma 2 reca la fattispecie autonoma aggravata dall'evento dannoso[43].
A ben vedere, la mancanza di un evento in senso giuridico non osterebbe alla configurazione di un evento in senso naturalistico, rilevante ai fini dell'art. 9 cod. pen., dal momento che la realtà esteriore risulterebbe comunque incisa dalla messa in pericolo del bene giuridico protetto. In questi termini, è possibile osservare che non mancherebbero tratti di collegamento con la legge nazionale.
Ma nei reati di pericolo astratto l'evento naturalistico si situa, in sostanza, nello stesso luogo della condotta, dalla quale rimane fondamentalmente indistinguibile, ben poco rivelando intorno alla direzione dell'astratta messa in pericolo e della direzione dell'offesa – sempre che il principio di offensività possa ritenersi rispettato[44].

---

[41] Cfr. MANTOVANI, *Diritto penale. Parte Speciale. II*, cit., 144; PICA G., *I reati nella società dell'informazione*, cit., 1010; MEZZETTI, *Reati contro il patrimonio*, cit., 350-351; NERI, *Criminologia e reati informatici*, cit., 88 ss.; FIANDACA-MUSCO, *Diritto penale. Parte speciale – Volume II, tomo secondo: I delitti contro il patrimonio*, Bologna, 2014, 148-149. PECORELLA, *Reati informatici contro il patrimonio*, cit., 289, sottolinea come la fattispecie in esame risulti modellata sulla falsariga di quella ai sensi dell'art. 420 cod. pen., che punisce l'attentato ad impianti di pubblica utilità, e ne sottolinea l'originalità, rispetto alle altre norme presenti nel codice – insieme a quella di cui all'art. 635-*quinquies* – quanto all'elemento della pubblica utilità.

[42] Cfr. MEZZETTI, *Reati contro il patrimonio*, cit., 350, il quale nega decisamente che il comma 2 dell'art. 635-*quinquies* cod. pen. possa configurare una circostanza aggravante, con l'effetto che il danno così cagionato è sottratto al bilanciamento fra circostanze di cui all'art. 69 cod. pen.

[43] Cfr. MEZZETTI, *Reati contro il patrimonio*, cit., 352-353, il quale peraltro condivisibilmente critica con vigore la parificazione dei limiti edittali fra art. 635-*ter* ed art. 635-*quinquies* cod. pen., dovendosi ritenere la messa in pericolo di dati sicuramente meno grave rispetto a quella di un intero sistema informatico; FIANDACA-MUSCO, *Diritto penale. PS II 2*, cit., 150-151.

[44] Cfr. FIORE C., FIORE S., *Diritto penale. Parte generale*, cit., 196-201, in particolare 198. Nella giuri-

Tuttavia, non sempre appare agevole collegare la "pubblica utilità" di un sistema informatico, qualora quest'ultimo sia accessibile da ambiti geografici diversi e lontani fra di loro, con l'interesse di un gruppo di persone localizzato in un determinato ambito nazionale.
Esso è senz'altro possibile quando si parla, per esempio, di *software* o sistemi connessi alla sorveglianza di un luogo[45] o all'utilità di enti radicati in un territorio o nell'amministrazione di uno Stato – come, per esempio, le banche dati di giurisprudenza – mentre è molto più complesso quando tale sistema sia legato ad entità sovranazionali, internazionali, o ad entità associative o commerciali senza una sede fisica rilevante ai fini del reato commesso in concreto. L'anticipazione della soglia di rilevanza penale rende peraltro difficile individuare anche *quale collettività* sia stata astrattamente posta in pericolo.
La trattazione di analoghe figure di reato in altri ordinamenti – per tutti, quello tedesco – non verrà svolta in questa sede, dal momento che si ritiene che esse possano rappresentare un interessante spunto ai fini delle prospettive *de jure condendo*.
3.3. *I reati informatici in senso lato o* computer crimes. Per quanto concerne i reati commessi *per mezzo* delle reti telematiche, ma diretti a beni giuridici differenti rispetto alla sicurezza dei sistemi e delle comunicazioni informatici, è possibile osservare casi di reati di pericolo astratto che non consentono la determinazione di uno o più soggetti passivi[46].
Uno dei casi più significativi, a tal riguardo, si è presentato nel contesto dell'ordinamento tedesco, in relazione ai reati di opinione connessi al sostegno di teorie revisioniste della *Shoah*, sussumibili nel reato di "sobillazione delle masse" (*Volksverhetzung*) di cui al § 130 *StGB*[47].

---

sprudenza costituzionale, sul tema si è registrato l'arresto costituito dalla Sentenza n. 333 del 1991.
[45] Per tutte, cfr. Cass., Sez. II Pen., Sentenza 14 marzo 2012 n. 9870, CED Rv 252465: nel caso di specie, il sistema telematico danneggiato di pubblica utilità è il sistema di videocamere di sorveglianza di una Procura della Repubblica.
[46] TIEDEMANN, *Wirtschaftsstrafrecht. Einführung und Allgemeiner Teil*, cit., 173, presenta la questione della criminalità informatica soprattutto nell'ottica delle truffe transnazionali commesse per il tramite informatico.
[47] Testo originale della disposizione:
» *(1) Wer in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören,*
1. gegen eine nationale, rassische, religiöse oder durch ihre ethnische Herkunft bestimmte Gruppe, gegen Teile der Bevölkerung oder gegen einen Einzelnen wegen seiner Zugehörigkeit zu einer vorbezeichneten Gruppe oder zu einem Teil der Bevölkerung zum Hass aufstachelt, zu Gewalt- oder Willkürmaßnahmen auffordert oder
2. die Menschenwürde anderer dadurch angreift, dass er eine vorbezeichnete Gruppe, Teile der Bevölkerung oder einen Einzelnen wegen seiner Zugehörigkeit zu einer vorbezeichneten Gruppe oder zu einem Teil der Bevölkerung beschimpft, böswillig verächtlich macht oder verleumdet,

wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft.
(2) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer
1. eine Schrift (§ 11 Absatz 3) verbreitet oder der Öffentlichkeit zugänglich macht oder einer Person unter achtzehn Jahren eine Schrift (§ 11 Absatz 3) anbietet, überlässt oder zugänglich macht, die
a) zum Hass gegen eine in Absatz 1 Nummer 1 bezeichnete Gruppe, gegen Teile der Bevölkerung oder gegen einen Einzelnen wegen seiner Zugehörigkeit zu einer in Absatz 1 Nummer 1 bezeichneten Gruppe oder zu einem Teil der Bevölkerung aufstachelt,
b) zu Gewalt- oder Willkürmaßnahmen gegen in Buchstabe a genannte Personen oder Personenmehrheiten auffordert oder
c) die Menschenwürde von in Buchstabe a genannten Personen oder Personenmehrheiten dadurch angreift, dass diese beschimpft, böswillig verächtlich gemacht oder verleumdet werden,
2. einen in Nummer 1 Buchstabe a bis c bezeichneten Inhalt mittels Rundfunk oder Telemedien einer Person unter achtzehn Jahren oder der Öffentlichkeit zugänglich macht oder
3. eine Schrift (§ 11 Absatz 3) des in Nummer 1 Buchstabe a bis c bezeichneten Inhalts herstellt, bezieht, liefert, vorrätig hält, anbietet, bewirbt oder es unternimmt, diese Schrift ein- oder auszuführen, um sie oder aus ihr gewonnene Stücke im Sinne der Nummer 1 oder Nummer 2 zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen.
(3) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer eine unter der Herrschaft des Nationalsozialismus begangene Handlung der in § 6 Abs. 1 des Völkerstrafgesetzbuches bezeichneten Art in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören, öffentlich oder in einer Versammlung billigt, leugnet oder verharmlost.
(4) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer öffentlich oder in einer Versammlung den öffentlichen Frieden in einer die Würde der Opfer verletzenden Weise dadurch stört, dass er die nationalsozialistische Gewalt- und Willkürherrschaft billigt, verherrlicht oder rechtfertigt.
(5) 1Absatz 2 Nummer 1 und 3 gilt auch für eine Schrift (§ 11 Absatz 3) des in den Absätzen 3 und 4 bezeichneten Inhalts. 2Nach Absatz 2 Nummer 2 wird auch bestraft, wer einen in den Absätzen 3 und 4 bezeichneten Inhalt mittels Rundfunk oder Telemedien einer Person unter achtzehn Jahren oder der Öffentlichkeit zugänglich macht.
(6) In den Fällen des Absatzes 2 Nummer 1 und 2, auch in Verbindung mit Absatz 5, ist der Versuch strafbar.
(7) In den Fällen des Absatzes 2, auch in Verbindung mit Absatz 5, und in den Fällen der Absätze 3 und 4 gilt § 86 Abs. 3 entsprechend.«

Traduzione, a cura dello scrivente:

«(1) Chiunque, in un modo che sia idoneo a turbare la pace pubblica,
1. istighi all'odio contro un gruppo nazionale, razziale, religioso o contrassegnato tramite la propria provenienza etnica, contro parti della popolazione o contro un singolo a causa della sua appartenenza ad uno dei gruppi predetti o ad una parte della popolazione, o esorti ad azioni violente o di sopraffazione, ovvero
2. contesti la dignità umana altrui ingiuriando, rendendo intenzionalmente sospetti o calunniando uno dei predetti gruppi, parti della popolazione o un individuo a causa della sua appartenenza ad essi
è punito con la reclusione da mesi tre ad anni cinque.
(2) È punito con la reclusione fino a 3 anni o con la multa chiunque
1. diffonda, reda accessibile al pubblico o offra, conceda o renda accessibile ad una persona minore degli anni diciotto uno scritto (§ 11 co. 3 *StGB*) che
a) istighi all'odio contro un gruppo designato ai sensi del co. 1 n. 1, contro parti della popolazione o contro un singolo a causa della sua appartenenza a uno dei gruppi o parti di popolazione predetti;
b) esorta a comportamenti violenti o prevaricatori contro le persone di cui alla lett. *a*);
c) contesti la dignità umana delle persone di cui alla lett. *a*) ingiuriandole, rendendole intenzionalmente sospette o calunniandole;

Il caso può essere riassunto come segue: l'autore della condotta, dedito alla diffusione di teorie revisioniste della *Shoah* per mezzo di un sito internet, era un soggetto nato in Germania ed emigrato in Australia in giovane età, diventando cittadino di tale Stato. Egli tornava in seguito nel Paese natale per compiere studi storici per poi ritrasferirsi in Australia. L'immissione dei dati inerenti alle teorie revisioniste veniva pertanto effettuata dal territorio australiano[48].

Nel caso si specie, le problematiche in esame presentano in un elevato grado di complessità: il soggetto attivo e il server si trovavano in Australia; la condotta è criminalizzata in Germania; non era possibile ravvisare uno o più soggetti passivi direttamente interessati dalla condotta, dal momento che essa consisteva essenzialmente nella diffusione al pubblico, tramite un sito *internet*, di pur deprecabili opinioni.

La soluzione adottata è stata quella di collocare il *locus commissi delicti* in Germania, considerando quale elemento di collegamento, molto estensivamente, il fatto che il sito recante le teorie revisioniste fosse accessibile anche

---

2. renda accessibile ad una persona minore degli anni diciotto o al pubblico, mediante l'uso della radio o di mezzi telematici, uno dei contenuti di cui al n. 1, lett. da *a*) a *c*);

3. produca, consegni, conservi, offra, reclamizzi o si impegni a introdurre o esporre i suddetti scritti, al fine di utilizzarli in tutto o in parte ai fini indicati dai nn. 1 e 2 o di consentirne una tale utilizzazione da parte di un'altra persona.

(3) È punito con la reclusione fino a 5 anni o con la multa chiunque, pubblicamente o nel corso di un'assemblea, approvi, neghi o minimizzi una condotta commessa nel corso del regime nazionalsocialista che sia sussumibile nel § 6 del *Völkerstrafgesetzbuch* [lett. "codice penale internazionale", atto di recepimento dello Statuto di Roma, *ndt*] in un modo che sia idoneo a perturbare la pace pubblica.

(4) È punito con la reclusione fino a 3 anni o con la multa chiunque, pubblicamente o nel corso di un'assemblea, perturbi la pace pubblica in una modalità lesiva della dignità umana della vittima approvando, negando o minimizzando la violenza o il totalitarismo nazionalsocialisti.

(5) Il comma 2, nn. 1 e 3, vale anche per uno scritto (§ 11 co. 3 *StGB*) che abbia il contenuto indicato nei commi 3 e 4. In base al comma 2, n. 2, è punito chi rende accessibile ad una persona minore degli anni diciotto o al pubblico un contenuto del tipo di quello indicato nei commi 3 e 4 per mezzo della radio o di mezzi telematici.

(6) Il tentativo è punibile in relazione ai casi di cui al comma 2, nn. 1 e 2, anche in combinato con il comma 5.

(7) Il § 86 co. 3 *StGB* [riproduzione o proposizione di strumenti di propaganda anticostituzionali scriminate dal fine artistico o scientifico, *ndt*]si applica ai casi di cui al comma 2, anche in combinato con il comma 5, nonché in quelli di cui ai commi 3 e 4».

[48] La sentenza vertente sul caso è *BGH, 1. Strafsenat, Urteil vom 12. Dezember 2000, 1 StR 184/00*, pubblicata nella raccolta ufficiale delle pronunce del *Bundesgerichtshof* in materia penale - *BGHSt*, vol. 46 (2000), 212 ss.

In dottrina, nella manualistica, SATZGER, *Internationales und Europäisches Strafrecht*, cit., 61 ss.; RENGIER, *Strafrecht AT*, cit., 35. Nella letteratura specifica, LAGODNY, *BGH, 12. 12. 2000 – 1 StR 184/00. „Auschwitzlüge" auf einem ausländischen Server im Internet*, in *JuristenZeitung*, 23/2001, 1194-1200; SATZGER, *StR Das deutsche Strafanwendungsrecht*, cit.

da utenti tedeschi. Essa è evidentemente improntata dalla necessità di non lasciare impunito un fatto al quale l'opinione pubblica tedesca è diventata molto sensibile negli ultimi decenni.
In modo analogo si pongono, come sottolineato da autorevole dottrina italiana, alcune manifestazioni del cd. cyberterrorismo: segnatamente, quelle volte alla propagazione di idee di lotta, al reclutamento di nuove leve per l'associazione terroristica e alla ricerca di finanziatori per il tramite di *internet*. Simili figure delittuose, prive peraltro di una previsione normativa dedicata ai relativi *computer crimes* e quindi fondate sulle figure di terrorismo "comune" (artt. 270-*quater* ss. cod. pen.), puniscono la formazione delle associazioni in un momento molto anticipato dell'*iter criminis*. Esso finisce per risultare prodromico non solo agli attentati, ma addirittura alla preparazione degli stessi.
I soggetti passivi di siffatte figure di reato non sono rinvenibili, non potendosi considerare tali – in alcuni casi, opinabilmente – i destinatari dei messaggi, del reclutamento e delle richieste di finanziamento ed essendo le condotte punite in un momento ancor lontano dalla stessa concretizzazione del pericolo[49].
3.4. *Le dimensioni del problema*. La trattazione fin qui svolta consente di circoscrivere ulteriormente il problema connesso ai reati informatici a soggetto passivo indeterminato.
L'assenza di soggetti passivi univocamente determinati o determinabili rende arduo collegare l'evento ad un'unica legge penale nazionale. Bisogna infatti considerare la difficoltà di collocare con esattezza la lesione di sistemi informatici "di pubblica utilità" o le lesioni derivanti, per esempio, da reati di opinione nell'ambito di un territorio statale piuttosto che in un altro, essendo tali beni difficili da "nazionalizzare" attraverso il collegamento ad un unico ambito territoriale[50].
Rilevano poco, a tal fine, la titolarità formale del sistema o il luogo di registrazione del dominio. Il soggetto formalmente titolare di un sistema informatico danneggiato o messo in pericolo, come si è precisato, potrebbe essere diverso da quelli i cui diritti vengano violati dalla condotta, specie nel caso in cui il titolare stesso sia un soggetto impersonale e l'utilità esplicata dal sistema vada a vantaggio di una pluralità di persone. Il luogo di registrazione di un dominio informatico è una procedura formale che serve ad attribuire un nome ad un sito *web* o ai servizi di *hosting* della corrispondenza *email*: nulla rivela

[49] Cfr. FLOR, *Cyber-terrorismo e diritto penale in Italia*, cit., 354-359.
[50] Il riferimento alle politiche di "nazionalizzazione" dei beni giuridici protetti è criticato puntualmente da SGUBBI, *Il reato come rischio sociale*, Bologna, 1990, 16-17.

sull'estensione dell'areale nel quale verranno veicolati i messaggi elettronici e i dati in essi contenuti.
In aggiunta, non può essere d'aiuto ricorrere alla massima estensione del principio di territorialità data dal legame con un qualsiasi atto che rivesta «un significato apprezzabile nell'ambito del fatto considerato *ex post* nella interezza del suo svolgimento»[51], potendosi in tal modo il collegamento del fatto ulteriormente frazionare in una molteplicità di ordinamenti.
A fortiori, il principio della personalità passiva, com'è evidente, non appare in tale ambito risolutivo. Né risulta applicabile quello della personalità attiva, non rientrando i reati cui si è fatto riferimento nelle enumerazioni tassative delle categorie che consentono di ricorrervi.
Tali soluzioni, nella loro applicazione più classica, non si prestano a risolvere casistiche del tipo di quelle presentate. Si rende necessario, a tal fine, uno sforzo interpretativo ulteriore, volto a superare i limiti che una normativa dal tradizionale ancoraggio territoriale può manifestare rispetto ad una materia che, oltre a denotare la deterritorializzazione menzionata in apertura, non offre possibilità di "fisicizzazione" dell'evento.
4. *Possibili soluzioni* de jure condito. Non appare possibile, *allo stato dell'arte*, dare una risposta univoca e universalmente valida alla complessa questione che, con questo contributo, si intende porre[52].
Le soluzioni percorribili in relazione a reati i cui soggetti passivi siano individuabili rimangono di fatto quelle la cui applicazione ha l'effetto di "recidere il nodo di Gordio" ai fini di attivare gli strumenti processuali per ricercare e perseguire i soggetti attivi. Basandosi, essenzialmente, sul rinvenimento di *alcuni* soggetti a vario titolo danneggiati o messi in pericolo, esse ricorrono a delle forzature per collocare il *locus commissi delicti* nel luogo in cui il soggetto passivo percepisce il danno.
Tuttavia, si può osservare la loro efficacia ai fini di evitare una situazione di persistente impunità dell'autore del fatto e nell'evitare conflitti di legge applicabile, di giurisdizione nonché, sul piano del diritto processuale interno, di competenza. I medesimi intenti, a ben vedere, devono rappresentare l'obiettivo principale anche delle soluzioni concernenti i reati informatici a soggetto passivo indeterminato.
Nel contesto della dottrina tedesca si sono proposte diverse soluzioni, tutte

[51] In questi termini ROMANO M., *Commentario sistematico al codice penale. Parte generale*, Milano, II ed. 1995, 110.
[52] Così anche SATZGER, *Internationales und Europäisches Strafrecht*, cit., 64.

basate sull'interpretazione del § 9 *StGB*[53]. Esse sono agevolmente analizzabili anche alla luce del diritto penale italiano.

4.1. *Il luogo del potenziale pericolo concreto*. La prima di esse, a carattere estensivo, ricorrendo all'evento come elemento di collegamento, fissa il *locus commissi delicti* nel luogo nel quale il pericolo astratto avrebbe potuto realizzarsi nella successiva esplicazione di un danno in concreto[54]. A tale criterio si è ispirata la Corte federale tedesca nel decidere sul caso delle tesi negazioniste diffuse via internet[55].

Una simile teoria, tuttavia, non può che portare ad un'eccessiva dilatazione del concetto di *locus commissi delicti* in base alle esigenze dell'ordinamento che in concreto persegua un determinato fatto di reato.

4.2. *Il luogo al quale la condotta è indirizzata*. L'eccessiva arbitrarietà del criterio di collegamento del "luogo del pericolo potenziale" ha condotto a concepire soluzioni basate sul legame oggettivo con un determinato territorio, facendo riferimento al luogo al quale la condotta sia "finalisticamente indirizzata". Tale elemento sarebbe desumibile, per esempio, dalla lingua utilizzata.

Tale soluzione poco s'adatta al problema principale che concerne i reati informatici a soggetto passivo determinato, il quale, giova ribadire, è la generale deterritorializzazione delle condotte in rete con l'aggiunta – appunto – della non identificabilità di un soggetto passivo determinato. A quale luogo, infatti, si potrà collegare un reato di opinione integrato da un articolo redatto in lingua inglese?

4.3. *Il luogo dell'inserimento dei dati*. Altre soluzioni hanno tentato di far leva sulle tradizionali categorie del principio della personalità attiva.

La proposta dottrinale più raffinata, in tal senso, è quella che ha tentato di scindere il profilo del luogo in cui il soggetto attivo concretamente agisce da quello in cui si realizzi la condotta descritta dalla fattispecie di reato. Fonte

---

[53] Per un quadro completo e sintetico sul tema, cfr. SATZGER, *op. ult. cit.*, 63.

[54] Cfr. JOFER, *Strafverfolgung im Internet. Phänomenologie und Bekämpfung kriminellen Verhaltens in internationalen Computernetzen*, Berlin, 1997, 108.

[55] Massima della sentenza: *„Stellt ein Ausländer von ihm verfaßte Äußerungen, die den Tatbestand der Volksverhetzung im Sinne des § 130 Abs. 1 oder des § 130 Abs.3 StGB erfüllen (‚Auschwitzlüge'), auf einem ausländischen Server in das Internet, der Internetnutzern in Deutschland zugänglich ist, so tritt ein zum Tatbestand gehörender Erfolg (§ 9 Abs.1 3.Alternative StGB) im Inland ein, wenn diese Äußerungen konkret zur Friedensstörung im Inland geeignet sind"*. Traduzione, a cura dello scrivente: «Qualora uno straniero diffonda in *Internet* dichiarazioni da lui redatte, che integrano il fatto tipico di incitamento al popolo ai sensi del § 130 comma 1 o comma 3 dello StGB ("Menzogna su Auschwitz"), tramite un server straniero accessibile da utenti tedeschi di *Internet*, si verifica nel territorio tedesco un evento appartenente al fatto tipico (§ 9 comma 1 terza alternativa *StGB*) nel momento in cui tali affermazioni siano concretamente idonee a rappresentare un pericolo per la pace in Germania». Per la dottrina v. *retro*, nota 48.

d'ispirazione di tale modello sono le tecnologie basate sull'introduzione dei dati rispetto ad un determinato ambito nazionale o sulla loro diffusione all'estero: la prima fonda il collegamento con la legge nazionale dello Stato in cui i dati sono introdotti[56].

Un orientamento analogo è quello seguito dalla giurisprudenza di legittimità italiana ai fini di fissare il *locus* della diffamazione per il tramite di *internet* laddove non sia individuabile una vittima concreta e, di conseguenza, il luogo di consumazione dell'evento[57] (solitamente rinvenuto là dove il soggetto passivo percepisce l'offesa[58]), determinando in tal modo la competenza territoriale.

Questa soluzione appare senz'altro la più intelligente se si ha riguardo allo *status quo*, ma presenta comunque il difetto di indebolire eccessivamente i profili di offensività, anche in relazione a reati di pericolo, che può essere collegato alla mera introduzione di dati in un certo ambito nazionale[59]. A ciò s'aggiunga la possibilità, per gli *hacker* più esperti, di far disperdere le tracce dell'indirizzo IP dal quale hanno agito, nascondendolo o "spacchettandolo" su più personal computer diversi.

Soprattutto, essa non appare applicabile ai *cyber crimes* basati sull'intercettazione dei dati dai sistemi informatici messi sotto attacco, qualora tale intercettazione non avvenga tramite virus.

4.4. *Considerazioni critiche*. La situazione analizzata comporta, inevitabilmente, che in termini di legge applicabile e di giurisdizione competente non potrà che valere la regola fattuale sintetizzata dagli anglosassoni nel prosaico detto *early bird catches the first worm*, per evitare discussioni che protraggano una situazione di incertezza e di indecisione – nel fugace crimine transnazionale, è più che mai valido l'adagio liviano *dum Romae consulitur, Saguntum expugnatur*. La prima procura ad avviare l'azione penale[60], il primo ente esponenziale (per esempio, associazioni di consumatori o di utenti) a occuparsi della

---

[56] La teoria è stata formulata da SIEBER, *Internationales Strafrecht im Internet. Das Territorialitätsprinzip der §§ 3, 9 StGB im globalen Cyberspace*, in *Neue Juristische Wochenschrift*, 29/1999, 2065-2072, spec. 2068.

[57] Cfr., *ex plurimis*, Cass., Sez. V Pen., Sentenza 21 luglio 2015 n. 31677, CED Rv 264521 – 01 (Pres. G. Lapalorcia, Rel.-Est. P.G. Demarchi Albengo): «*Nei reati di diffamazione tramite la rete "internet", ove sia impossibile stabilire il luogo di consumazione del reato e sia stato invece individuato quello in cui il contenuto diffamatorio è stato caricato come dato informatico, per poi essere immesso in rete, la competenza territoriale va determinata, ai sensi dell'art. 9, primo comma, cod. proc. pen., in relazione al luogo predetto, in cui è avvenuta una parte dell'azione*».

[58] Cfr., *ex plurimis*, Cass., Sez. V Pen., Sentenze 25 luglio 2006 n. 25875, CED Rv 234528-01, e 14 giugno 2012 n. 23624, CED Rv 252964-01.

[59] Cfr. SATZGER, *Internationales und Europäisches Strafrecht*, cit., p. 64.

[60] Si noti il possibile parallelismo con i criteri suppletivi indicati dall'art. 9 cod. proc. pen.

querela e/o della denuncia[61] finiranno per avere un ruolo decisivo nel definire chi perseguirà gli autori di reati informatici a soggetto passivo indeterminato di dimensione transnazionale e, in termini sostanziali, quale legge sarà ad essi applicabile.

In un simile contesto, l'avvio simultaneo o differito di più azioni penali in più Stati diversi è questione tutt'altro che accademica. La risoluzione del problema non potrà che essere raggiunta sulla scorta degli strumenti di cooperazione internazionale in materia penale – particolarmente rapidi ed efficienti in seno all'Unione Europea, decisamente più farraginosi nel contesto del diritto internazionale "classico", che richiede necessariamente il ricorso ad estradizioni e rogatorie – e sulla base di un corretto ricorso al *ne bis in idem*, cui la Carta EDU (art. 6 implicitamente, art. 14 co. 7 PIDCP *expressis verbis*) e la CDFUE (art. 50) hanno attribuito valore di diritto fondamentale dell'essere umano.

Una simile situazione lascia ovviamente uno spazio eccessivo all'alea. A tal riguardo sarebbe sufficiente avanzare considerazioni riguardanti il livello di civiltà giuridica, gli indirizzi dottrinali e giurisprudenziali, le norme di diritto interno di ciascuno degli ordinamenti statali coinvolti.

È evidente che, nel contesto di uno scenario futuro sempre più dominato dalla tecnologia, radicata come strumento della vita sia economica che sociale della società globale e dei singoli individui, non si può rimanere fermi ad uno *status quo* come quello raffigurato.

Il crimine informatico è destinato ad occupare, infatti, una porzione sempre più importante del traffico investigativo e giudiziario: esso non può essere fermato da confini o politiche restrittive; inoltre, sarà sempre più orientato alla vittimizzazione di massa, prima ancora che alle lesioni monosoggettive.

5. *Prospettive* de jure condendo. Alla luce delle considerazioni fin qui svolte, appare evidente che il problema dei reati informatici a soggetto passivo indeterminato imponga di concepire soluzioni *de jure condendo*, puntando a prevenire future situazioni di *impasse* fra diversi ordinamenti, destinate altrimenti ad aumentare, e a superare quelle già esistenti.

La questione della individuazione di un parametro normativo di collegamento tra il crimine informatico a soggetto passivo indeterminato e legislazione nazionale necessita di un intervento normativo da esplicarsi a più livelli. Essendo ormai evidente l'insufficienza di riforme delle legislazioni penali nazionali, pur per certi versi necessarie, terreno d'elezione di simili prospettive do-

[61] Sul fondamentale ruolo degli enti collettivi in relazione al processo vertente sui reati a soggetto passivo indeterminato, cfr. DE VITA, *I reati a soggetto passivo indeterminato*, cit., 437 ss.

vranno essere l'ordinamento dell'Unione Europea e il diritto internazionale[62].
La dottrina, invero, non manca di offrire alcune proposte già compiutamente formulate. L'analisi critica delle stesse potrà recare suggerimenti ai fini della formulazione di proposte ulteriori.
5.1. *La proposta dell'istituzione di una Corte penale internazionale per i crimini di* Internet. Si è ipotizzata l'istituzione di una Corte internazionale – o comunque di una sezione speciale della Corte penale internazionale – dedicata precipuamente ai reati informatici[63]. Sembra invero agevole poter escludere fin da subito l'utilità di una simile soluzione.
Essa, infatti, pur essendo apparentemente in grado di risolvere il problema che in questa sede si è analizzato, non solo si scontra con i problemi tipici del diritto internazionale – *in primis*, il fatto che tale ipotetica Corte potrebbe operare solamente in collaborazione con gli Stati che firmino l'eventuale convenzione *ad hoc*, accettando figure di reato pressoché uniformi a livello planetario; oppure sulla base della consuetudine internazionale[64], al momento di difficile individuazione rispetto alla criminalità informatica – ma per giunta non appare neanche una soluzione in linea con quella che è la *ratio* dell'esistenza delle Corti penali internazionali.
Esse, infatti, sono preposte innanzitutto a giudicare crimini espressione di una "macro-criminalità" di apparato di stampo politico, militare e/o etnico, quantunque sia astrattamente possibile una loro commissione individuale[65]. Si tratta di fatti idonei a turbare l'ordine internazionale, nonché a ledere o esporre a pericolo beni giuridici di fondamentale importanza per la vita di un cospicuo numero di esseri umani o per intere comunità statali o nazionali. Le vittime, pertanto, sono normalmente categorizzabili, a loro volta, in gruppi etnici, politici o militari ben identificabili[66].

---

[62] Cfr. PICOTTI, *Quale diritto penale nella dimensione globale del* cyberspace*?*, FORNASARI, WENIN (a cura di), *Diritto penale e modernità*, cit., il quale a pp. 312-316 sottolinea la necessità che il confronto *muova* dalle istanze sovranazionali in modo da fornire regole certe e condivise al *Cyberspace*, sottolineando al contempo la possibilità di rispettare la funzione di garanzia del diritto penale tramite lo strumento del recepimento da parte dei parlamenti nazionali.
[63] Latore di una proposta in tal senso è, *inter alios*, SCHJOLBERG, *Potential new global legal mechanisms on combating cybercrime and global cyberattacks*, Relazione al Convegno *ISPAC*, cit. (v. *retro*, nota 9) propone un *Drafi* di Statuto per una siffatta Corte.
[64] Cfr. VON ARNAULD, *Völkerrecht*, Heidelberg, 2012, 509.
[65] Cfr. CONFORTI, *Diritto internazionale*, Napoli, VIII ed. 2010, 206 ss., 208.
[66] A tal proposito, sembra decisamente poco equivocabile la disposizione dell'articolo 5 dello Statuto di Roma: «*The jurisdiction of the Court shall be limited to the most serious crimes of concern to the international community as a whole*». Il principio è comunemente accettato in diritto internazionale: CONFORTI, *op. et loc. ult. cit.*; VON ARNAULD, *Völkerrecht*, cit., 506-507, che pone la questione in termini della spettanza alla comunità internazionale del diritto alla punizione (*Strafanspruch*).

Simili fattispecie non sono adeguatamente giudicabili dalle Corti nazionali[67], come d'altronde insegnano alcuni precedenti storici[68].
Al contrario, è agevole osservare che le condotte dei reati informatici, anche qualora assumano rilevanza transnazionale, normalmente non arrivano a porre in pericolo beni giuridici di un rilievo paragonabile a quelli protetti dalle norme penali internazionali, né un insieme di soggetti passivi del medesimo ordine di grandezza.
Le fattispecie di crimine internazionale sono peraltro dirette, in via di norma, al contrasto di fatti commessi da soggetti non organici ad un sistema politico o militare. Per quanto concerne i reati informatici, invece, l'unica ipotesi in cui venga seriamente in rilievo una commissione di natura organica è quella della responsabilità da reato degli enti, materia a sua volta oggetto delle giurisdizioni nazionali[69].
A tal proposito, è possibile osservare che eventuali ipotesi di illeciti commessi tramite mezzi informatici e sussumibili nelle fattispecie previste dallo Statuto di Roma – in altri termini, *computer crimes* internazionali – o dirette a ledere sistemi informatici di primaria importanza per l'ordine pubblico internazionale, come possono essere quelli di organizzazioni internazionali o di altri Stati, rientrerebbero comunque nella giurisdizione della Corte penale internazionale[70].

---

[67] Cfr. KREß, *Völkerstrafrecht in Deutschland*, in *Neue Zeitschrift für Strafrecht*, 12/2000, 617-626, in part. 626, e SATZGER, *Internationales und Europäisches Strafrecht*, cit., 236 ss., per i profili più generali sulle Corti penali internazionali; GILLESPIE, *Cybercrime*, cit., 26, più specificamente sulla proposta di una Corte *ad hoc* (o sezione *ad hoc*) per i crimini informatici. Per quanto riguarda i reati di competenza della Corte penale internazionale, si veda innanzitutto il Terzo Preambolo dello Statuto di Roma, che fa riferimento a «*such grave crimes threaten the peace, security and well-being of the world*»; per le singole fattispecie, Artt. 6-8 *bis*.

[68] Cfr. K. VON LINGEN, *„Crimes Against Humanity" Eine umstrittene Universalie im Völkerrecht des 20. Jahrhunderts*, in *Zeithistorische Forschungen*, 3/2011, 373 ss., 378 ss..

[69] Nel diritto italiano, tale forma di responsabilità è prevista dall'art. 24-bis del decreto legislativo 8 giugno 2001, n. 231. A tal proposito NERI, *Criminologia e reati informatici*, cit., 147-150. Nel diritto tedesco, le fattispecie che verranno trattate *infra*, par. 5.3, sono applicabili agli enti a titolo di responsabilità penale-amministrativa in combinato disposto con la previsione del § 30 del *Ordnungswidrigkeitengesetz* (*OWiG*).

[70] Un'analisi completa e approfondita del problema è quella proposta da DITTMAR, *Angriffe auf Computernetzwerke.* Ius ad bellum *und* ius in bello, Berlin, 2015. Tale Autore, infatti, alle pp. 38 ss. prospetta la possibilità di attacchi mossi a reti di computer (*Computernetzwerke*) predisposte a fini di sicurezza nazionale ed internazionale, per scopi militari e per scopi finanziari, riconducendo tuttavia il tema alla violazione di norme di diritto internazionale e prospettando (58 ss.), al fine di prevenire le degenerazioni che potrebbero rendere necessarie l'intervento della Corte penale internazionale, anche le soluzioni diplomatiche o sanzionatorie da adottare in sede di dialogo intergovernativo o di Assemblea generale delle Nazioni Unite.
Una prospettiva più sintetica dal punto di vista degli ordinamenti penali nazionali è offerta da SARZANA

Vi è un altro aspetto di rilievo. L'edificazione di un sistema di responsabilità penale internazionale per i *cybercrimes* ed i *computer crimes* comporterebbe, in relazione ad essi, anche l'adozione del principio di universalità della giurisdizione penale. In base ad esso, il soggetto attivo potrebbe essere giudicato in qualsiasi Stato del Mondo egli venga rinvenuto e tradotto innanzi ad un giudice[71] Sulla base delle medesime ragioni che inducono ad escludere l'utilità e la concreta ipotizzabilità di una Corte internazionale per i crimini informatici, sembra il caso di affermare che una simile acquisizione non sarebbe né ragionevole né praticabile.

Al di fuori di simili casistiche, peraltro non così agevoli da ipotizzare, le giurisdizioni nazionali con le quali il fatto di reato informatico possa presentare un collegamento continuano a offrirsi come la sede naturale dei procedimenti aventi ad oggetto reati informatici, pur con le questioni teoriche e le evidenti difficoltà di ordine pratico che non si è mancato di porre in evidenza.

5.2. *La proposta dell'applicazione al diritto penale della soluzione di cui alla Direttiva UE in materia di* E-Commerce. Una soluzione particolarmente interessante e meritevole di considerazione è quella proposta ispirandosi alla Direttiva sull'E-Commerce, 2000/31/CE.

Essa si ispira al principio dello Stato di stabilimento dell'operatore economico in regime di commercio su internet (art. 20)[72], per cui, ovunque sia commessa la condotta o si verifichi l'evento, questi risponderà delle infrazioni commesse ai sensi della legge dello Stato in cui ha posto la propria sede, che si impegna a sua volta a sanzionarlo. Trasponendo una simile soluzione in diritto penale, si potrebbe optare per l'applicazione della legge nel luogo in cui il soggetto attivo risieda oppure, in assenza di una residenza effettiva, dimori[73].

Un tale criterio di collegamento, al momento pressoché sconosciuto dal diritto penale, può senz'altro costituire un'innovazione valida ed efficace nel contesto dell'Unione Europea, contribuendo a realizzare anche sul *web* quello spazio di sicurezza e di giustizia che essa, istituzionalmente, si prefigge di

---

DI S. IPPOLITO, *Informatica, internet e diritto penale*, cit., 7-24.

[71] CONFORTI, *Diritto internazionale*, cit., 210; VON ARNAULD, *Völkerrecht*, cit., 505.

[72] Testo della norma, dedicata alle sanzioni per l'adozione di pratiche commerciali contrarie a quelle indicate come corrette dalla direttiva: «Gli Stati membri comminano sanzioni per la violazione delle norme nazionali di attuazione della presente direttiva e prendono tutti i provvedimenti necessari per la loro applicazione. Le sanzioni devono essere effettive, proporzionate e dissuasive».

[73] Cfr. SATZGER, *Internationales und Europäisches Strafrecht*, cit., 65-66. Sembra augurarsi una soluzione nel medesimo senso anche TIEDEMANN, *Wirtschaftsstrafrecht. Einführung und Allgemeiner Teil*, cit., p. 172.

creare.
Una simile innovazione meriterebbe, peraltro, di essere estesa il più possibile anche a livello internazionale mediante lo strumento trattatistico, ricorrendo a strumenti di cogenza e/o ad accordi *ad hoc* in relazione agli Stati non firmatari al fine di evitare il più possibile la creazione di "paradisi per criminali informatici".
La proposta in esame sconta, tuttavia, lo svantaggio di tempi di realizzazione che appaiono tutt'altro che rapidi: considerando solamente il livello di ordinamento dell'Unione Europea, al tempo necessario per l'approvazione di una direttiva in materia, infatti, si aggiungerebbe quello necessario per il recepimento della stessa nei singoli ordinamenti nazionali nonché, eventualmente, quello delle procedure d'infrazione nei confronti degli Stati membri che non adempiano entro il termine. Oltrepassando i confini dello Spazio Europeo, al di là del quale la prospettata direttiva non avrebbe vigenza, è evidente che la stipula di trattati richiederebbe tempi ed impegno ulteriori, specie laddove si riscontrassero situazioni di Stati reticenti ad applicare il principio della residenza dell'operatore e che magari pensino di trarre profitto da tale possibilità.
Ne consegue la necessità di concepire *medio tempore* soluzioni che garantiscano risultati adeguati, o quantomeno il miglioramento dello *status quo*, in tempi più brevi e con minori ostacoli, mantenendo tuttavia in vita questo ambizioso e valido progetto sul lungo termine.
5.3. *Soluzioni a breve termine per gli ordinamenti interni. La parte generale del diritto penale*. Gli ordinamenti nazionali dovrebbero pertanto impegnarsi a garantire soluzioni in tempi più rapidi, pur con l'inevitabile limite della vigenza delle norme e dell'*enforcement* procedurale limitato al territorio nazionale – facendo salvo il ricorso, come già si è detto, a strumenti di collaborazione processuale come il mandato d'arresto europeo o l'estradizione.
Almeno due sono le direttrici lungo le quali si può agire: *in primis*, l'introduzione di norme *ad hoc* nella parte generale ai fini della fissazione del *locus commissi delicti* per i reati informatici; in secondo luogo, un riordino della parte speciale, in modo da dare ordine al microsistema dei singoli reati informatici.
Partendo, in questa sede, dalla parte generale, una norma come l'Art. 113-2-1 del *Code pénal* rappresenterebbe una soluzione utile a consacrare il legame fra soggetto passivo e vittima ai fini della legge applicabile.
Questo non risolve le questioni connesse ai reati informatici a soggetto passivo indeterminato – in particolare, per quanto riguarda i reati comuni com-

messi tramite il mezzo informatico o *computer crimes* – che abbiano una dimensione transnazionale. A tal fine, seppure in via provvisoria, conviene aderire alla proposta di punire il reato informatico nel luogo in cui sia avvenuto, in tutto o in parte, l'inserimento dei dati[74], conferendo una veste espressa a tale principio – in virtù della particolarità del settore sul quale incide e della sua possibile eccentricità rispetto alle regole di determinazione del *locus commissi delicti* – nel contesto norme di parte generale.

5.4. (segue) *I* cybercrimes *della parte speciale ed il corretto recepimento della Convenzione di Budapest. Il modello tedesco*. Gli adattamenti della parte generale, in materia di contrasto alla criminalità informatica, avrebbero ben poca efficacia se non ci si curasse a dovere di migliorare la qualità della parte speciale. I *cybercrimes*, nel codice penale italiano, non costituiscono un sistema vero e proprio, né esso sarebbe agevolmente rinvenibile senza gli sforzi della dottrina.

Tuttavia, come anticipato, altri Stati firmatari della convenzione possono offrire soluzioni interessanti – seppur non esenti da critiche – ai fini di un riordino della materia. In parte, come già affermato dalla dottrina, la strada sarebbe già stata tracciata dalla Convenzione di Budapest, un cui fedele recepimento avrebbe evitato la formazione delle principali aporie normative: in particolare l'art. 6, che avrebbe richiesto la criminalizzazione del possesso di strumenti *principalmente* intesi a pratiche illecite e di sistemi di accesso ottenuti contro la volontà del titolare o responsabile. Il dolo specifico di commettere i reati informatici, nella previsione di tale norma, avrebbe dovuto accedere a tale base di fatto, senza essere l'unico, reale elemento selettivo della fattispecie[75].

---

[74] Cfr. SIEBER, *Internationales Strafrecht im Internet*, cit., 2065 ss.

[75] Testo dell'art. 6 della Convenzione:

Article 6 – Misuse of devices

1. *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 and without right:*

a) the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in para-

A tal proposito, un ordinamento che ha perseguito una soluzione interessante è quello tedesco[76]. Nel contesto dello *StGB*, i reati che sono stati inseriti a seguito sono contenuti o nel Titolo quindicesimo sui reati contro la riservatezza personale (*Fünfzehnter Abschnitt. Verletzung des persönlichen Lebens- und Geheimbereichs*) o nel ventisettesimo, concernente i reati di danneggiamento (*Siebenundzwanzigster Abschnitt. Sachbeschädigung*).
Accanto ad un sistema di cinque figure di reati di evento-danno – spionaggio di dati (*Datenausspähen*, § 202a), captazione di dati (*Abfangen von Daten*, § 202b) e ricettazione di dati (*Datenhehlerei*, § 202d) nel quindicesimo titolo, modificazione illecita di dati (*Datenveränderung*, § 303a) e sabotaggio di computer (*Computersabotage*, § 303b) nel ventisettesimo – il legislatore tedesco ne ha istituita una sola di pericolo astratto, dedicata alla preparazione (*Vorbereiten*) degli altri reati (§ 202c) e alla copertura di una lacuna di sistema che lasciava impunite molte condotte di hackeraggio[77]. Tale disposizione rinvia alle altre figure contenute nel medesimo titolo, eccetto quella di cui al § 202d; quelle contenute fra i reati di danneggiamento, a loro volta rinviano al § 202c.
La disposizione recita:
[§ 202c *StGB*] (1) *Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er*
1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,
herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

---

graph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph (1 a. ii) of this article.
Si richiama anche in questa sede PICOTTI, *La ratifica della Convenzione Cybercrime*, cit., il quale ha ricordato come una fattispecie come quella di cui all'art. 635-*ter* cod. pen. avrebbe potuto assumere connotati decisamente più rispettosi del principio di offensività se il legislatore si fosse correttamente attenuto alle indicazioni di cui all'art. 6 della Convenzione. Osservazioni analoghe vengono mosse da SCHUH, *Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz*, Berlin, 2012, 60-62, per introdurre l'analisi del § 202c *StGB*.
[76] Un'opera che si segnala per chiarezza ed organicità, a tal riguardo, è appunto SCHUH, *op. ult. cit.*
[77] Cfr. SCHUH, *op. cit.*, 60-61; J-P. GRAF, *§ 202c StGB*, in AA. VV., *Münchener Kommentar zum Strafgesetzbuch. Band 4*, III ed. 2017, *Randnummer* (di seguito *Rn*) 2-3.

(2) *§ 149 Abs. 2 und 3 gilt entsprechend.*
[Traduzione, a cura dello scrivente] Chi prepara un fatto di reato ai sensi dei §§ 202a o 202b, producendo, procurando a sé stesso o ad altri, vendendo, concedendo ad altri, diffondendo o rendendo comunque accessibili
1. password o analoghi codici di sicurezza, che consentono l'accesso ai dati (§ 202a co. 2), oppure
2. programmi per computer, il cui scopo è la commissione di tali fatti,
è punito con la reclusione non superiore ad anni due o con la multa.
(2) La disposizione di cui al § 149, commi 2 e 3, vale ai fini della presente.
Nel confronto con la normativa italiana, pur simile nel linguaggio e nei contenuti[78], è evidente che una simile soluzione garantisca un maggior ordine ed eviti una superfetazione di sistema con fattispecie pressoché ripetitive; ha, inoltre, il vantaggio di collegare la *ratio* della fattispecie di pericolo astratto a quelle di evento, garantendo in buona sostanza il rispetto del principio di offensività e l'anticipazione della punibilità in una reale ottica di prevenzione del danno. Il richiamo al secondo e al terzo comma del § 149 *StGB*, inoltre, garantisce l'impunità del fatto qualora il soggetto attivo desista o receda dalla preparazione dei reati in preparazione[79].
Tale norma sconta, tuttavia, alcune incertezze che si sono segnalate anche a riguardo della fattispecie di cui all'art. 615-*quinquies* cod. pen.: quella della criminalizzazione di mezzi dei quali sarebbe possibile un uso in sé lecito[80] e il conseguente ruolo decisivo del dolo specifico per selezionare i fatti penalmente rilevanti[81].
Il superamento di questa criticità, che quindi accomuna il § 202c alle norme del codice penale italiano, richiederebbe pertanto di criminalizzare la mera disponibilità di dispositivi informatici potenzialmente dannosi solo laddove l'uso illecito sia, se non l'unico possibile, quantomeno quello suggerito dalla fisiologia del dispositivo stesso. In tutti gli altri casi, una strutturazione della fattispecie rispettosa della finalità garantista del diritto penale e del principio di offensività richiederebbe, invece, di portare la soglia di punibilità a manifestazioni di pericolo concreto, in modo da prevenire comunque potenziali of-

[78] Cfr. SCHUH, *op. cit.*, 62- 63; GRAF, *op. cit.*, *Rn* 8-16.
[79] Cfr. SCHUH, *op. cit.*, p. 63; GRAF, *op. cit.*, *Rn* 34-35.
[80] Cfr. SCHUH, *op. cit.*, 63 ss.: l'Autore sottolinea che anche atti di interpretazione autentica rilasciati dal *Bundestag* – in particolare, la *Drucksache* 16/3656 del 30 novembre 2016 – vadano nel senso di richiedere la penalizzazione del possesso di strumenti anche in sé leciti. La giurisprudenza costituzionale tedesca, sul punto, avrebbe apportato correttivi soltanto parziali, richiedendo l'obiettiva manifestazione del dolo specifico.
[81] Cfr. SCHUH, *op. cit.*, 63-64; GRAF, *op. cit.*, *Rn* 30-31.

fese di massa e individuando i potenziali soggetti passivi.
Una criticità che non viene superata dalla soluzione testé richiamata, ad ogni modo, è quella della "diaspora" delle fattispecie di *cybercrimes* in diverse sub-partizioni codicistiche, le quali richiamerebbero le figure tradizionali cui i reati informatici appaiono assimilabili.
Ben lungi dal ritenere una simile soluzione condivisibile, infatti, sarebbe invece opportuno prendere atto della particolarità dei reati riguardanti le comunicazioni informatiche, senza contestualizzarli impropriamente nelle tipologie delittuose tradizionali che, con qualche forzatura, il singolo legislatore possa considerare come più vicine al bene giuridico tutelato. Il tema del *locus commissi delicti*, specie in relazione a fattispecie di pericolo astratto che non consentano la determinazione del soggetto passivo, dimostra in modo paradigmatico le ragioni e le necessità sottese ad una categorizzazione *ad hoc* e al discostamento dai beni giuridici tradizionali.
6. *Conclusioni.* Traendo le fila del discorso, sembra possibile affermare che le direttrici che dovranno necessariamente improntare la politica legislativa del contrasto alla criminalità informatica, sia da parte dei legislatori interni che in sede di organismi sovranazionali, potrebbero essere riassunte nei termini che seguono.
In primis, in presenza di un soggetto passivo determinato, in quanto tale possibile titolare di un diritto al risarcimento, si dovrebbe favorire il collegamento del fatto di reato informatico mediante norme di "fisicizzazione", che pongano l'evento nel luogo in cui si trova il soggetto passivo medesimo. Questa è la soluzione attuata in Francia mediante l'Art. 113-2-1 del *Code pènal*, come più volte ribadito; si può istituire un parallelo con il criterio di individuazione della competenza territoriale che in Italia si adopera, a livello di diritto processuale penale, per individuare il giudice naturale chiamato a giudicare sulla diffamazione diretta ad un soggetto determinato[82].
Quando invece si versi nel caso di reati a soggetto passivo indeterminato, sarà opportuno ricorrere, in un primo tempo, al pur non sempre efficace criterio del *locus* nel quale i dati, in tutto o in parte, sono stati inseriti. A tale riforma della parte generale se ne potrebbero aggiungere, ai fini di un miglioramento

[82] Così *ex plurimis* Cass., Sez. V Pen. (Presidente P. Savani, Est.-Rel. A. Guardiano), Sentenza 29 luglio 2016 n. 33287, CED Rv. 267703 – 01: «*Il reato di diffamazione, non consistente nell'attribuzione di un fatto determinato, commesso a mezzo di trasmissione televisiva diffusa in diretta su tutto il territorio nazionale si consuma al momento della percezione del contenuto offensivo dell'altrui reputazione da parte di soggetti diversi dall'agente e dalla persona offesa, per cui la competenza territoriale appartiene al giudice del territorio in cui si è verificata la percezione del messaggio offensivo contenuto nella trasmissione televisiva*».

complessivo del sistema, altre di parte speciale: strutturare quali fattispecie di pericolo astratto, a soggetto passivo indeterminato, solo quelle nelle quali gli strumenti informatici utilizzati abbiano quale scopo principale la commissione di illeciti; riformare la criminalizzazione del possesso di strumenti informatici di cui siano possibili e fisiologici anche usi leciti conferendo alle relative fattispecie la veste di reato di pericolo concreto; ricondurre le fattispecie di *cybercrimes* in un titolo loro dedicato, ricorrendo a sub-partizioni secondarie per individuare altri beni giuridici potenzialmente coinvolti da suddetti reati.
Sul lungo termine sarà il caso di assicurare, comunque, la punizione del soggetto attivo nel luogo in cui egli risiede o dimora, superando così i limiti connessi agli altri criteri. Tale risultato sarà da perseguirsi tramite l'emanazione di direttive per gli Stati membri dell'Unione Europea e, per quelli che non ne siano membri, per mezzo dello strumento convenzionale.
Quest'ultima soluzione, in particolare, si presenta come del tutto innovativa e per certi versi originale rispetto alla tradizione del diritto penale, ma potrebbe consentire di raggiungere obiettivi molto ambiziosi nel contrasto alla criminalità informatica.
Di un *Internet* più sicuro e meno incline a offrirsi quale porto franco per la commissione di reati, specie transnazionali, ne potranno beneficiare categorie molto ampie della popolazione mondiale, con benefici immancabili anche per lo sviluppo economico e sociale dell'umanità.