NOMINA NUDA TENEMUS?
LO STATUTO PENALISTICO DEL CRIMINE INFORMATICO TRA MUTAMENTI FENOMENICI E MODIFICAZIONI SEMANTICHE

dis CRIMEN articoli
3.1.2023

Gaia Fiorinelli[*]

NOMINA NUDA TENEMUS?
THE REGULATION OF COMPUTER CRIMES BETWEEN PHENOMENAL CHANGES AND SEMANTIC ADJUSTMENTS.

The article aims to offer a critical perspective on the interpretative approach adopted in the Italian system by legislators and judges when dealing with computer crimes. Indeed, this phenomenon is still often regarded with a certain degree of uncertainty by interpreters, sometimes postulating its full equivalence to what happens in physical reality, other times conversely arguing its absolute and enduring novelty: thus, sometimes analogical reasoning and metaphorical images constitute the only justification for the application of one regime or another, while we argue that only an approach oriented on the actual function and functioning of information technologies should determine the definition or selection of the applicable law. To this end, some examples are given – drawn from legislative provisions and judgments – to show how metaphorical thinking can improperly influence the legal conceptualization of new technologies.

KEYWORDS Cyberlaw – Cybercrime – Analogical Reasoning – Metaphorical Language – Dynamic Interpretation

1. Premessa: lo scopo dell'indagine

Il presente lavoro si propone di offrire una prospettiva critica sull'approccio interpretativo del legislatore e della giurisprudenza al fenomeno della criminalità

[*] Assegnista di ricerca in diritto penale nella Scuola Superiore Sant'Anna di Pisa.

informatica *lato sensu* intesa, muovendo dalla constatazione che – a oltre vent'anni dalla Convenzione del Consiglio d'Europa sulla criminalità informatica siglata a Budapest nel 2001 e alle soglie dell'introduzione di una Convenzione internazionale delle Nazioni Unite sul contrasto all'uso delle tecnologie dell'informazione e della comunicazione per finalità criminali[1], ma soprattutto nell'era della digitalizzazione pressoché totale[2] – tale fenomeno sia, nell'ordinamento interno, tuttora spesso riguardato con certo grado d'incertezza, a volte postulandosene la piena sovrapponibilità all'*equivalente analogico*, altre volte per converso predicandosene l'assoluta e perdurante *novità*.

Si tratta, a ben vedere, di un binomio *tipico* del diritto (penale) dell'informatica: non certo perché si tratti dell'*unico* settore chiamato a confrontarsi con qualcosa di nuovo, ma perché – semplificando, se non banalizzando la questione – la rivoluzione digitale nasce in effetti dalla *codifica*, dalla *riproduzione virtuale* della realtà fisica[3], cosicché è naturale (ma anche necessario) che tale strutturale *somiglianza* porti a domandarsi, di volta in volta, se ci si trovi o meno in presenza di qualcosa di realmente *nuovo*, anche ai fini della definizione del diritto applicabile. Tuttavia, come si dirà, nel rispondere a un tale quesito sono spesso estensioni analogiche (talora azzardate) e immagini metaforiche a costituire l'unica giustificazione per l'applicazione di un regime o di un altro, senza che, invece, sia un approccio orientato sull'effettiva *funzione* e sull'effettivo *funzionamento* delle tecnologie informatiche a determinare la costruzione o la selezione del diritto applicabile.

Lo scopo dell'indagine è, dunque, duplice: anzitutto, dopo aver ricostruito il più tradizionale dibattito dottrinale in ordine al *modo* di regolare il fenomeno tecnologico (nello specifico, il crimine informatico) – nella strutturale alternativa tra regolazione *ex novo* e applicazione del diritto esistente, che in effetti costituisce "il dilemma dei dilemmi" nell'ambito della *cyberlaw* – si proporrà una diversa impostazione di

[1] Si allude alla risoluzione dell'Assemblea Generale delle Nazioni Unite del 27 dicembre 2019, n. 74/247, «*Countering the use of information and communications technologies for criminal purposes*», con la quale è stato costituito un *«Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes»*. Al riguardo, v. anche A. MATTARELLA, *La futura Convenzione ONU sul* cybercrime *e il contrasto alle nuove forme di criminalità informatica*, in *www.sistemapenale.it*, 11 marzo 2022.

[2] Osservano ad esempio A. GARAPON, J. LASSEGUE, *La giustizia digitale. Determinismo tecnologico e libertà,* trad. it., Il Mulino, 2021, 79, come, con la progressiva estensione dell'«ambito del calcolabile a tutta la realtà umana» le tecnologie informatiche e digitali abbiano ormai assunto le dimensioni di un «fatto sociale totale».

[3] Nel senso che la trasformazione *digitale* si fonda sulla codifica «sotto forma di numeri» di «eventi del mondo fisico» cfr. ancora A. GARAPON, J. LASSEGUE, *La giustizia digitale. Determinismo tecnologico e libertà*, cit., 43 ss.

metodo, mediante un rovesciamento di prospettiva che invita a riflettere prima di tutto sulla novità del *fatto*, anziché sulla novità del *diritto*; sulla base di tali premesse, si tenterà poi di "decodificare" le tecniche di "costruzione giuridica" della tecnologia adottate tanto dal legislatore, quanto nell'applicazione giurisprudenziale, al fine di comprendere a quali fattori si attribuisca rilievo per decidere se un dato fenomeno esiga un'apposita disciplina o possa invece contentarsi di una qualche disposizione già esistente (e, nel caso, di *quale*, tra le tante).

L'idea di fondo è che la regolazione (anche penalistica) di tale fenomeno – quello tecnologico, che ormai rappresenta un fattore costante e strutturale tanto nella commissione di reati, quanto nelle successive indagini e attività processuali – possa in effetti beneficiare (e necessiti) di un approccio pragmatico, che consenta di superare le incertezze applicative e le insidie di un linguaggio spesso metaforico, riguardando invece la *sostanza* (non già il *nome*) del *fatto* da regolare e così sciogliendo l'alternativa delineata nel titolo: e cioè se il mutamento sia meramente *semantico* (e così, ad esempio, la lettera e la *e-mail* si equivalgano, ai fini dell'applicazione di una determinata disciplina), oppure se il cambiamento sia *fenomenico* (e, dunque, per rimanere nell'esempio, la lettera e l'*e-mail* non si equivalgano affatto).

2. Il crimine informatico nel contesto della c.d. *cyberlaw*

Per impostare la riflessione secondo la traiettoria delineata, occorre allora anzitutto rilevare come l'impatto della rivoluzione informatica sul diritto sia tradizionalmente analizzato ricorrendo alla nota dicotomia – che si è sviluppata principalmente nella dottrina nord-americana in tema di *cyber-regulation* – tra "eccezionalismo" e "non-eccezionalismo" nell'approccio giuridico alle nuove tecnologie[4]. In buona

[4] La letteratura sul tema è sterminata; con riguardo alle coordinate fondamentali della contrapposizione tra *exceptionalists* e *unexceptionalists* nella dottrina nordamericana, cfr. J. L. GOLDSMITH, *Against Cyberanarchy*, *University of Chicago Law Occasional Paper*, 1999, n. 40; T. S. WU, *Cyberspace Sovereignty? – The Internet and the International System*, in *Harvard Journal of Law & Technology*, 1997, 10, 3, 647 ss.; T. S. WU, *Is Internet Exceptionalism Dead?*, in B. SZOKA, A. MARCUS (a cura di), *The Next Digital Decade: Essays on the Future of Internet*, Washington D.C., 2010, 179 ss.; D. R. JOHNSON, D. POST, *Law and Borders – The Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996, 48, 5, 1367 ss.; D. G. POST, *Against "Against Cyberanarchy"*, in *Berkeley Technology Law Journal*, 2002, 17, 1365 ss.; ID., *Governing Cyberspace: Law*, in *Santa Clara High Tech Law Journal*, 2007, 24, 4, 883 ss.; F. H. EASTERBROOK, *Cyberspace and the Law of the Horse*, in *University of Chicago Legal forum*, 1996, 207 ss.; L. LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, 1998. Nell'ordinamento italiano, cfr. ad es. R. FLOR, Cyber-criminality*: le fonti internazionali ed europee*, in A. CADOPPI, S. CANESTRARI,

sostanza, mentre gli "eccezionalisti" ritengono che la nuova realtà digitale presenti, rispetto alla tradizionale realtà materiale, caratteristiche distintive tali da giustificare – o persino da richiedere – un cambiamento nell'approccio anche in termini giuridici, i "non-eccezionalisti" sostengono, invece, che non vi sia, tra *cyberspace* e realtà materiale, alcuna differenza di rilievo tale da doverla valorizzare anche in una prospettiva giuridica: secondo quest'ultima impostazione teorica, infatti, ogni attività posta in essere nel *cyberspace* troverebbe nel mondo fisico un proprio "correlativo", un equivalente funzionale, e, di conseguenza, nel *cyberspace* non si porrebbe alcuna questione ulteriore e diversa, che non possa essere affrontata e risolta mediante il ricorso al diritto già esistente o, comunque, con un mero adattamento di strumenti regolativi già collaudati.

Come si anticipava già in premessa, una simile contrapposizione pare dipendere *a monte* da una diversa concezione del fenomeno tecnologico in sé considerato, che rappresenta per gli uni un mutamento *fenomenico* sostanziale – in quanto ciò che avviene *online* esisterebbe, in effetti, «solo in rete»[5], e in un modo tutto particolare – mentre costituisce per gli altri un mero cambiamento *modale* di "fatti" che nella sostanza rimangono inalterati: nel *cyberspazio*, in altri termini, le persone «diffamano, invadono la *privacy*, molestano, (…), concludono e violano contratti, distribuiscono materiale pornografico (…) infrangono marchi, violano i diritti d'autore, rubano dati» nello stesso modo in cui è sempre avvenuto «di persona, per telefono o per posta»[6].

Una simile divergenza di vedute si rinviene, del resto, anche nel più ristretto ambito del c.d. "diritto penale dell'informatica": mentre, infatti, numerosi studi di carattere criminologico hanno individuato nel *cybercrime* una *nuova* fenomenologia criminosa, caratterizzata da alcuni tratti distintivi[7], pare tuttora controverso e indefinito il significato che effettivamente si possa attribuire a tale categoria in termini prettamente *penalistici*. Invero, sul punto si contrappongono (almeno) due distinti approcci, tesi l'uno a rilevare la *novità* e la *molteplicità* delle questioni che si pongono nell'era di internet, e l'altro, invece, a ridimensionare l'effettivo impatto delle tecnologie informatiche sulle categorie tradizionali del diritto penale.

Semplificando (forse troppo) tali diverse posizioni teoriche, su un primo versante si possono collocare quanti ritengono che le questioni nuove che si pongono nell'era digitale abbiano essenzialmente un carattere pratico-applicativo, e debbano

A. MANNA, M. PAPA (diretto da), *Trattato di diritto penale – Cybercrime*, Torino, 2019, 143.

[5] D. R. JOHNSON, D. POST, *Law and Borders – The Rise of Law in Cyberspace*, cit., 1375.

[6] Cfr. J. L. GOLDSMITH, *Against Cyberanarchy*, cit., 1202.

[7] Cfr. J. CLOUGH, *Principles of Cybercrime*, Cambridge, 2010, 5 ss.; N. K. KATYAL, *Criminal Law in Cyberspace*, in *University of Pennsylvania Law Review*, 2001, 149, 1003 ss.

perciò essere affrontate, tutt'al più, mediante la riforma di taluni istituti processuali; con riguardo, invece, alla disciplina *sostanziale*, «alle condotte poste in essere nel "*cyberworld*" dovrebbero applicarsi le medesime leggi che già disciplinano tali condotte nel mondo fisico»[8] e la stessa nozione di "*cybercrime*" sarebbe tanto suggestiva quanto inutile[9].

Di ben diverso avviso è, invece, chi ritiene che l'impatto delle tecnologie informatiche sul diritto penale non possa ridursi a mere questioni di carattere applicativo, legate alle difficoltà pratiche di accertare e reprimere i *cybercrime*, dal momento che, al contrario, il crimine informatico si porrebbe in completa opposizione con le caratteristiche del diritto penale tradizionale, trattandosi di tutelare nuovi beni *intangibili* da minacce che si caratterizzano, in modo inedito, per la rapidità, l'anonimità e la portata globale[10] e, dunque, di affrontare fenomenologie criminose sostanzialmente diverse, potenzialmente caratterizzate da una rapidissima velocità di esecuzione e non più connotate da precisi vincoli di natura territoriale o spaziale[11].

[8] In tale prospettiva cfr. la ricostruzione di N. K. KATYAL, *Criminal Law in Cyberspace*, cit., 1003 ss., che riporta altresì la posizione in tal senso assunta dal Department of Justice degli Stati Uniti. Cfr. dunque, U.S. DEPT. OF JUSTICE, *The electronic frontier: the challenge of unlawful conduct involving the use of the internet*, Report, Marzo 2000. Si legge nel Report che: «*substantive regulation of unlawful conduct... should, as a rule, apply in the same way to conduct in the cyberworld as it does to conduct in the physical world. If an activity is prohibited in the physical world but not on the Internet, then the Internet becomes a safe haven for that unlawful activity*». Sottolinea, in particolare, i problemi di *enforcement,* T. J. HOLT, *Regulating Cybercrime through Law Enforcement and Industry Mechanisms*, in *The Annals of the American Academy of Political & Social Science*, 2018, 140 ss. In relazione alla sostanziale equivalenza funzionale tra attività online e offline, v. anche Y. NAZIRIS, *'A Tale of Two Cities' in three themes – A critique of the European Union's approach to cybercrime from a 'power' versus 'rights' perspective*, in *European Criminal Law Review*, 2013, 3, 319 ss.: «*the essence of criminal conduct –at least as regards a significant number of offenses against property and against the person- has remained the same, even though the means to carry it out are different*». In tal senso cfr. ancora O. S. KERR, *Computer Crime Law*, 4th ed., St. Paul, 2017. Cfr., infine, S. W. BRENNER, *Cybercrime Metrics: Old Wine, New Bottles?*, in *Virginia Journal of Law and Technology*, 2004, 13, 9, 2002 ss.: «*Online crime eludes these strategies, and in that regard it is truly distinguishable from traditional crime. Online criminals operate in the virtual world and are therefore not subject to the physical and territorial constraints that govern conduct in the real world*».

[9] Cfr. T. S. WU, *Cyberspace Sovereignty? – The Internet and the International System*, cit., 655.

[10] Cfr. in tal senso, ex multis, U. SIEBER, *Mastering Complexity in the Global Cyberspace*, in DELMAS-MARTY, PIETH, SIEBER (a cura di), *Les chemins de l'harmonization pénale*, Paris, 192 ss.; B. SANDYWELL, *On the globalisation of crime: the Internet and new criminality*, cit., 39, secondo il quale «*our normal categories of crime and criminality seem wholly inadequate*».

[11] Cfr. J. CLOUGH, *Principles of Cybercrime*, cit., 5 ss. ma anche R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), *Trattato di diritto penale* – Cybercrime, Milano, UTET, 2019, 141 ss.

In una posizione intermedia si pone, infine, chi ritiene che un approccio "eccezionalista" nel settore della criminalità informatica risulti validamente giustificato soltanto a condizione di circoscrivere in termini sufficientemente ristretti la nozione stessa di *cybercrime*: invero, lamentando la confusione che deriva dalla tendenza a considerare "informatico" ogni reato che, in vario modo, coinvolga l'uso delle nuove tecnologie, si è sottolineato come, effettivamente, per i reati "tradizionali" che vengano semplicemente posti in essere mediante l'uso di un *computer* o per i quali l'avvento di *internet* abbia creato nuove possibilità – nei quali, dunque, l'elemento "informatico" è meramente accidentale – si pongano soltanto difficoltà di carattere pratico e processuale, essendo invece necessario affrontare con disposizioni di carattere specifico soltanto quei reati che possano essere commessi *esclusivamente* nel *cyberspace*[12].

Anche nel contesto della dottrina penalistica italiana è possibile, dunque, riscontrare una tendenziale opposizione tra taluni Autori, i quali ritengono che le tecnologie dell'informazione e della comunicazione condizionino talune categorie generali del diritto penale, determinando «un'almeno parziale obsolescenza di contenuti essenziali di alcune tradizionali categorie dogmatiche della parte generale, bisognose di nuovi ridefinizioni concettuali»[13] e, per converso, altri Autori, i quali, pur condividendo l'esigenza di attribuire rilievo alle peculiarità delle attività poste in essere in rete, negano che nozioni quali, ad esempio, quelle di condotta o evento possano subire alcuna dilatazione, «diretta a comprendere ulteriori effetti collegati al funzionamento di internet e all'operato di ulteriori *server* o all'attività degli utenti»[14].

3. Le insidie del linguaggio metaforico nel diritto (penale) dell'informatica: il fenomeno tecnologico tra ciò che è e ciò che sembra

Come si è anticipato, al fine di acquisire una prospettiva "di sistema"

[12] Cfr. D. S. WALL, *What are Cybercrimes?*, in *Criminal Justice Matters*, 2005, 58, 20 s. Cfr. anche la ricostruzione di B. SANDYWELL, *On the globalisation of crime: the Internet and new criminality*, in Y. JEWKES, M. YAR (a cura di), *Handbook of Internet Crime*, Routledge, Abingdon-on-Thames, 2009, 46, che ha ritenuto che il *cybercrime* possa essere efficacemente suddiviso entro tre diverse categorie, in termini relazionali rispetto ai reati tradizionali: (i) attività criminose tradizionali, che sono espanse o facilitate dalle tecnologie informatiche; (ii) attività criminose che sono generalizzate e radicalizzate, dal ricorso alle tecnologie informatiche; (iii) attività criminose che sono create dalle nuove tecnologie informatiche.

[13] Cfr. L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (diretto da), *Trattato di diritto penale – Cybercrime*, Torino, 2019, 33 ss.

[14] Cfr. S. SEMINARA, *Internet (diritto penale),* in *Enciclopedia del Diritto,* Annali, VII, Milano, Giuffrè, 2014, 567 ss., 570.

nell'approccio interpretativo allo statuto penalistico del crimine informatico, pare anzitutto necessario sottoporre a un vaglio critico già la stessa contrapposizione tra eccezionalismo e non-eccezionalismo: se, infatti, quella appena descritta è la più tradizionale impostazione teorica utilizzata per inquadrare (anche) il tema della criminalità informatica, si è condivisibilmente sottolineato come tanto l'eccezionalismo quanto il non-eccezionalismo – nel rispondere alla questione essenziale se internet sia qualcosa di *nuovo* e, in quanto tale, richieda una disciplina *speciale* – poggino su un'implicita precomprensione del fenomeno da regolare, ovverosia sulla riconosciuta (o negata) identità *sostanziale* tra una determinata tecnologia e un qualcosa di già esistente, la cui disciplina possa (o meno) essere applicata estensivamente[15].

È, dunque, su tale presupposto logico che occorre soffermarsi: se, infatti, «la prima reazione del diritto a una nuova tecnologia e quella di cercare analogie capaci di spiegare perché questa nuova tecnologia possa» – o meno – «essere trattata in modo identico rispetto a una tecnologia già esistente»[16] deve essere proprio tale primo segmento del ragionamento, volto a comprendere cosa una nuova tecnologia *rappresenti* per il diritto, a costituire il punto centrale (anche se spesso trascurato) della riflessione.

In proposito, risulta allora di notevole utilità per la presente riflessione richiamare una serie di studi, nei quali la questione dei rapporti tra diritto ed evoluzione tecnologica è stata inquadrata da un'angolatura del tutto diversa, di tipo essenzialmente metodologico-interpretativo.

In particolare, tale alternativa analisi dei rapporti tra diritto e tecnologia muove dalla constatazione che, al fine di ricomprendere una nuova tecnologia entro un discorso giuridico già esistente, gli interpreti ricorrano – più o meno consapevolmente – a *similitudini* e *metafore*, funzionali a consentire la susseguente costruzione giuridica del fenomeno considerato[17]. L'utilizzo del linguaggio metaforico risponde, infatti, all'insopprimibile esigenza umana di approcciare ciò che è sconosciuto «movendo dalla conoscenza, ossia per metafore dalla realtà»[18]. Così, ad esempio: colui che viola il diritto d'autore *online* è un "pirata"; la possibilità di accedere a dati e servizi mediante

[15] Cfr. O. KERR, *The Problem of Perspective in Internet Law*, in *Georgetown Law Journal*, 2003, 91, 357 ss. e in part. 380.

[16] Cfr. in questi termini A. M. FROOMKIN, *The metaphor is the key: cryptography, the clipper chip, and the Constitution*, in *University of Pennsylvania Law Review*, 860.

[17] In generale, cfr. G. LAKOFF, M. JOHNSON, *Metaphors We Live By*, 1980, University of Chicago Press; D. SCHÖN, *Generative metaphor: A perspective on problem-setting in social policy*, in A. ORTONY (ed.), *Metaphors and Thought*, 1979, Cambridge University Press, 253 ss.

[18] Cfr. F. GALGANO, *Le insidie del linguaggio giuridico. Saggio sulle metafore nel diritto*, Il Mulino, 2010, 14.

una connessione ha reso internet una "nuvola" (*cloud*); chi cerca informazioni sul *Web* lo sta "navigando", un *software* dannoso per un sistema informatico è un "virus". L'utilizzo di un linguaggio metaforico è a tal punto frequente in questo ambito, che addirittura la stessa evoluzione del diritto delle nuove tecnologie è stata da taluno definita come la storia di una «battaglia tra metafore»[19]. Un'analoga tendenza si sta, del resto, ripresentando nel recente dibattito relativo alla regolazione dei *robot*, nel cui ambito il confronto spesso si concentra sull'esigenza di definire *cosa* essi rappresentino per il diritto: "strumenti", "animali", "persone", "schiavi"[20] ?

Se tale è la premessa, non deve sfuggire, tuttavia, che ogni metafora, pur essendo all'inizio un utile strumento per «liberare il pensiero», possa finire tuttavia per «soggiogarlo»[21]. Occorre, infatti, tener bene presente che, da un lato, qualsiasi metafora prescelta abbia il potere di colorare e controllare il nostro successivo modo di pensare al suo oggetto e, dunque, di inquadrare il relativo problema regolatorio[22]; dall'altro lato, *a monte*, che ogni operazione interpretativa di questo tipo sia un'operazione intuitiva e inevitabilmente soggettiva, perché la scelta dell'una o dell'altra metafora (posta la non identità tra gli oggetti) dipenderà da quali caratteristiche di una determinata tecnologia l'interprete ritenga intuitivamente come più importanti o essenziali[23].

Andare «a caccia di metafore», anche nell'ambito del diritto della tecnologia, non deve dunque apparire come «andare a caccia di farfalle»[24], ma deve invece rispondere alla fondamentale esigenza di comprendere e scovare le insidie connesse all'uso del linguaggio metaforico, derivanti dal rischio «di scambiare la metafora per la realtà»[25] o, detto altrimenti, di confondere un linguaggio puramente descrittivo con un linguaggio ascrittivo-prescrittivo.

---

[19] Cfr. in questi termini ad es. S. LARSSON, *Metaphors, law and digital phenomena: the Swedish pirate bay court case*, in *International Journal of Law and Information Technology*, 2013, 21, 354 ss.; ma anche P. OHM, *The Myth of the Superuser: Fear, Risk, and Harm Online*, in *University of California, Davis Law Review*, 2008, 41, 1327 ss.; in part. 1373: «*Internet law is often a battle of metaphors*».

[20] Cfr. ad es. R. CALO, *Robots as Legal Metaphors*, in *Harvard Journal of Law & Technology*, 2016, 30, 1, 209 ss.; M. LETA JONES, J. MILLAR, *Hacking Metaphors in the Anticipatory Governance of Emerging Technology: The Case of Regulating Robots*, in R. BROWNSWORD, E. SCOTFORD, K. YEUNG, *The Oxford Handbook of Law, Regulation and Technology*, OUP, 2017, 597 ss.

[21] Questo adagio è attribuito al *Justice* Benjamin Cardozo, che l'ha espressa nel caso *Berkey v. Third Avenue Railway Co.*, 244 N. Y. 84, 94, 155 N. E. 58, 61 (1926).

[22] Cfr. J. WOLFF, *Cybersecurity as Metaphor: Policy and Defense Implications of Computer Security Metaphors*, 2014 TPRC Conference Paper, su *ssrn.com*, 4.

[23] Cfr. J. WOLFF, *Cybersecurity as Metaphor*, cit., 3.

[24] Cfr. in questi termini F. GALGANO, *Le insidie del linguaggio giuridico*, cit.,19.

[25] Cfr. F. GALGANO, *Le insidie del linguaggio giuridico*, cit., 20.

Nel medesimo filone interpretativo, del resto, si può anche annoverare la riflessione di chi ha sottolineato come il diritto di internet di per sé costituisca (e si riduca a) una sostanziale questione metaforica, nota come il c.d. «problema della prospettiva»[26]. Al fine di sottolineare il carattere relativo di qualsiasi metafora prescelta per descrivere il web, si è, infatti, osservato come ciascun fenomeno connesso all'uso di internet possa essere rappresentato da almeno due distinte prospettive: da un lato, da una prospettiva *interna*, che corrisponde con la prospettiva dell'utente, il quale, nell'utilizzare la rete, percepisce il Web come un mondo virtuale; dall'altro lato, da una prospettiva *esterna*, che osserva la rete "da fuori" e che, quindi, la concepisce come l'insieme dei computer collegati globalmente, con le relative infrastrutture. Ad esempio, si pensi all'attività di navigare sul Web per effettuare acquisti: da una prospettiva interna, si tratta di un *fatto* che si "avvicina" all'attività di un utente che visita un negozio fisico, con le relative implicazioni in termini di qualificazione giuridica; da una prospettiva *esterna*, invece, il *fatto* può essere descritto in termini sensibilmente diversi, concentrandosi l'attenzione sul collegamento tra i server e sulla trasmissione elettronica di informazioni[27]. Com'è evidente, la qualificazione giuridica dell'attività svolta *online* non dipenderebbe tanto dalle caratteristiche oggettive del fenomeno da regolare, quanto invece dalla prospettiva che l'interprete ritenga di adottare tra le due, che risultano parimenti legittime e giustificate.

Tali considerazioni portano, dunque, a ritenere che – anche nel più ristretto ambito della criminalità informatica – il tema dei rapporti tra diritto e tecnologia sottenda alcune sostanziali questioni interpretative che la contrapposizione tra "eccezionalismo" e "non-eccezionalismo" rischia di lasciare in secondo piano. Pertanto, ancor prima di valutare *come* internet debba essere regolato, è essenziale comprendere (e spiegare) come esso *debba* o *possa* essere inteso nel discorso giuridico: il punto centrale della riflessione è quindi costituito dalla *concettualizzazione* delle tecnologie, al fine di poterle poi qualificare giuridicamente: «*stop and question how we arrive at the facts of the Internet before we apply law to it*»[28].

[26] Cfr. O. KERR, *The Problem of Perspective in Internet Law*, cit., 357 ss.

[27] Cfr. O. KERR, *The Problem of Perspective in Internet Law*, cit., 362 ss.

[28] Cfr. O. KERR, *The Problem of Perspective in Internet Law*, cit., 381. Nella dottrina italiana, si possono richiamare in termini generali le riflessioni di A. DI MARTINO, *Dalla regola per il caso al caso per la regola. Variazioni brevi e stravaganti sul concetto di «caso» (case, Kasus)*, in Aa. Vv., *Studi in onore di Lucio Monaco*, Urbino University Press, 2020, 357 ss., che sottolinea l'importanza essenziale del momento della «selezione di quello che i giuristi chiamano i fatti, vale a dire la narrazione specificamente giuridica di ciò che è accaduto nella realtà».

4. La disciplina speciale del *cybercrime* nell'ordinamento italiano: «*new wine in old bottles*»?[29]

Prendendo, dunque, a punto di riferimento quelle impostazioni teoriche che invitano a mettere in discussione anzitutto la prospettiva con la quale si individuano i *fatti*, prima ancora di concentrarsi sulla disciplina che a questi risulti applicabile, è dunque possibile proseguire nella riflessione, secondo le coordinate indicate in premessa, con l'intento di verificare come – tanto nella riflessione teorica quanto nell'applicazione pratica – l'enfasi sulla questione della "specialità" o "non specialità" di internet e della sua disciplina lasci spesso irrisolta o dia per scontata la preliminare questione definitoria.

Muovendo da un'analisi del diritto vigente, il legislatore italiano è intervenuto specificamente nell'ambito della criminalità informatica con la l. n. 547/1993[30] e poi con la successiva l. n. 48/2008[31], al fine di adeguare l'ordinamento interno rispettivamente alla prima *Raccomandazione* del Consiglio d'Europa[32] e alla Convenzione di Budapest[33].

Pur trattandosi di interventi legislativi ampi ed eterogenei – finalizzati all'introduzione e alla modifica di numerose disposizioni di carattere sostanziale e processuale – è significativo osservare, nella prospettiva metodologica delineata, come il legislatore italiano, pur considerando «indispensabile una *specifica* regolazione del fenomeno», abbia tuttavia ritenuto che la particolarità della materia non costituisse ragione sufficiente per «la configurazione di uno specifico titolo»[34] e la costituzione di "un'area di tutela" a sé stante, decidendo, dunque, di strutturare la nuova disciplina semplicemente estendendo in via legislativa l'ambito applicativo di fattispecie di reato già esistenti e consolidate[35].

---

[29] Il titolo è una parafrasi del titolo del saggio di S. W. Brenner, *Cybercrime Metrics: Old Wine, New Bottles?*, in *Virginia Journal of Law and Technology*, 2004, 13, 9, 2002 ss.

[30] Rubricato «*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*».

[31] Che costituisce ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica.

[32] Cfr. la *Recommendation no. R (89) 9* del Comitato dei Ministri agli stati Membri sul *Computer-Related Crime*, adottata dal Comitato dei Ministri il 13 settembre 1989 al 428esimo incontro dei Deputati dei Ministri.

[33] Convenzione sulla criminalità informatica del Consiglio d'Europa, adottata a Budapest il 23 novembre 2001.

[34] Relazione del Disegno di legge n. 2773, presentato dal Ministro di Grazia e Giustizia. – "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica" (XI Legislatura, divenuto Legge 23 dicembre 1993, n. 547).

[35] Cfr. ancora la Relazione del Disegno di legge n. 2773.

Secondo quanto si legge nella *Relazione* di accompagnamento alla l. 547/1993, si decise, infatti, di «ricondurre i nuovi reati alle figure già esistenti che ad essi, pur nella loro autonomia, *appaiano più vicine*», giacché «le figure da introdurre sono apparse subito soltanto quali nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici (patrimonio, fede pubblica, eccetera) già oggetto di tutela nelle diverse parti del corpo del codice»[36]. Benché, dunque, il legislatore italiano sia intervenuto adottando una disciplina *speciale*, dedicata alla criminalità informatica, è tuttavia evidente che la scelta di modellare la nuova disciplina ricorrendo a una sorta di "analogia legislativa", volta a ricomprendere casi "nuovi" all'interno di fattispecie di reato "tradizionali", sottintenda (e dia per scontata) la presunta "vicinanza" tra le nuove ipotesi da regolare e i paradigmi di incriminazione preesistenti.

Non si possono, dunque, non condividere le riflessioni di chi ha ritenuto che tale *modus operandi* abbia costituito un limite «alla completa comprensione ed enucleazione delle particolarità della realtà di cui ci si occupa»[37]: su un piano lessicale, infatti, «l'attaccamento rituale alle formule tradizionali ha talora nuociuto alla messa a fuoco di tratti originali della nuova fenomenologia»[38] e, più in generale, la scelta di preservare la coerenza sistematica del codice si è tradotta nell'eccessiva "artificiosità" di alcuni segmenti della disciplina.

Su tali premesse, si analizzeranno ora alcuni esempi, al fine di verificare quali implicazioni siano derivate dalla scelta del legislatore penale di regolare internet "per analogia": si vedrà, in particolare, come tale impostazione metodologica abbia avuto sia implicazioni *particolari* (nel caso di singole fattispecie di reato, fortemente conformate dall'immagine prescelta dal legislatore), sia implicazioni di carattere *generale*, perché la scelta di ricondurre la disciplina del crimine informatico a molteplici "figure" già presenti nel codice ha prodotto l'effetto di disarticolare la nozione stessa di *cybercrime*, privando tale concetto di una qualsivoglia autonomia sistematica.

4.1. - *Lo "strano caso" del domicilio informatico*

Paradigmatica delle possibili contraddizioni e limitazioni discendenti

[36] Cfr. ancora la Relazione del Disegno di legge n. 2773 e C. PECORELLA*, Il diritto penale dell'informatica*, Padova, CEDAM, 2006.

[37] Cfr. F. BERGHELLA, R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, 9, 2329 ss.

[38] Cfr. ancora F. BERGHELLA, R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, cit., 2329 ss.

dall'approccio prescelto dal legislatore italiano è, ad esempio, la disciplina che è stata introdotta al fine di fornire una tutela penale *speciale* e *dedicata* avverso quei comportamenti di «*access without right to a computer system or network by infringing security measures*», ovverosia di accesso abusivo a sistema informatico, secondo quanto indicato nel *Report* allegato alla *Raccomandazione* n. 89 (9) del Consiglio d'Europa[39].

Nel panorama comparatistico si sono in effetti sviluppati molteplici modelli di tutela della sicurezza e della protezione di un sistema informatico: tra i più diffusi, secondo quanto si apprende da uno studio sul tema, vi sarebbe anche quello costruito sulla metafora dello «scassinatore»[40], del *burglar*, il ladro d'appartamento, ovverosia colui che s'introduce nell'altrui domicilio. Tale metafora sarebbe pervasiva nell'ambito della sicurezza informatica perché attraverso un binomio problema-soluzione ben familiare essa consentirebbe d'inquadrare (e conseguentemente risolvere) un problema nuovo: appunto, la sicurezza e la protezione di uno spazio virtuale (il sistema informatico), da concepirsi come se si trattasse di uno spazio fisico (il domicilio).

Tuttavia, com'è stato osservato, un simile approccio potrebbe non essere realmente efficace per «fornire indicazioni significative su come proteggere al meglio i sistemi informatici», perché tanto le condotte di attacco quanto le strategie di difesa differiscono di fatto sensibilmente, che si tratti di violare la «fortificazione di un castello» ovvero le misure di sicurezza di un *personal computer*[41]. Lo stesso vale, del resto, per le altre metafore più diffuse in questo ambito, quella della "guerra" (c.d. *cyberwar*, spesso usata quale immagine per rappresentare la sicurezza informatica e le strategie di difesa nell'ambito della politica internazionale) e quella della "malattia" (icasticamente rappresentata dalla configurazione dei programmi di manipolazione di un sistema informatico come un "*virus*"), le quali – a loro volta – non soltanto implicano una diversa concettualizzazione del problema della sicurezza informatica, ma soprattutto determinano differenti (e spesso implicite) conseguenze, quanto alla selezione del "modello" giuridico d'intervento ritenuto più opportuno[42]: ad esempio, è intuitiva la differenza tra la dimensione in un caso *individuale* e nell'altra *collettiva*, implicate dal ricorso ora alla metafora del domicilio, ora alla metafora della *cyberwar*.

[39] Cfr. CONSIGLIO D'EUROPA, *Computer-Related Crime. Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems*, 1990, reperibile su *oas.org,* in part. 49 ss.

[40] Cfr. J. WOLFF, *Cybersecurity as Metaphor*, cit., 6 ss.

[41] Cfr. ancora J. WOLFF, *Cybersecurity as Metaphor*, cit., 6-7.

[42] Cfr. ancora J. WOLFF, *Cybersecurity as Metaphor*, cit., 9 ss.

Ebbene, il legislatore italiano ha appunto deciso di concepire tale nuova incriminazione assimilando il sistema informatico al "domicilio" e perciò estendendovi la relativa protezione penale: invero, sul presupposto per cui «i sistemi informatici o telematici […] costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione»[43], si è introdotto – com'è noto – l'art 615-*ter* c.p., rubricato «Accesso abusivo a un sistema informatico o telematico» all'interno della Sezione IV («Dei delitti contro la inviolabilità del domicilio») del Capo III («Dei delitti contro la libertà individuale») del Titolo XII («Dei delitti contro la persona») del codice penale[44].

La scelta del legislatore italiano di ricorrere alla metafora del *domicilio*, per modellare la tutela del sistema informatico, ha tuttavia avuto ripercussioni di non poco momento: come si è osservato, se tale scelta può apparire suggestiva sul «piano delle simbologie e delle metafore», è sul piano «dei beni e degli interessi concreti»[45] – ovverosia, sul piano che propriamente dovrebbe interessare la politica criminale – che tale similitudine si rivela assai meno convincente.

Notevoli sono, infatti, i risvolti pratici della metafora prescelta dal legislatore: la collocazione sistematica della disposizione, ricompresa tra i "Delitti contro la persona" aveva, ad esempio, indotto alcuni interpreti a escludere che la norma incriminatrice punisse le condotte di indebita intrusione all'interno di sistemi informatici di interesse pubblico, «privi di qualunque contenuto personalistico e privatistico»[46]; del resto, esclusa tale eventualità nella prassi interpretativa, non pare nemmeno del tutto giustificata l'equiparazione che così si realizza tra sistemi informatici *privati* e *pubblici*, i quali sono entrambi tutelati sul modello del *domicilio* pur sottendendo interessi, esigenze di tutela e dimensioni offensive sicuramente diversi (e che ora trovano riconoscimento nella sola previsione della circostanza aggravante di cui al co. 3 dell'art. 615-*ter* c.p., per il caso in cui il sistema informatico sia *di interesse pubblico*).

[43] Cfr. ancora la Relazione del Disegno di legge n. 2773.

[44] Nella sezione relativa ai *delitti contro l'inviolabilità del domicilio* sono state collocate le fattispecie di cui agli artt. 615-*ter* c.p. (*Accesso abusivo ad un sistema informatico o telematico*), 615-*quater* c.p. (*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*), e 615-*quinquies* c.p. (*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*), tutte modellate sulla fattispecie generale di "Violazione di domicilio" ma punite – almeno avuto riguardo alla pena-base – meno gravemente rispetto alle analoghe fattispecie relative al "domicilio fisico".

[45] Cfr. ancora F. BERGHELLA, R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, cit., 2329 ss.

[46] Cfr. ancora F. BERGHELLA, R. BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, cit., 2329 ss.

Ancora, si è osservato come il richiamo al paradigma del domicilio sia peraltro fuorviante, perché contraddetto dalla previsione, nel disposto dell'art. 615-*ter* c.p., che il sistema informatico o telematico oggetto di accesso abusivo debba essere «protetto da misure di sicurezza»: tale requisito escluderebbe, infatti, che i sistemi informatici siano protetti *di per sé stessi*, semplicemente in quanto «estensione della sfera privata», e a prescindere dall'esistenza e dall'efficacia delle misure di sicurezza predisposte dal titolare, come invece accade per il domicilio fisico (il quale è «tutelato sempre e non soltanto quando il titolare abbia apprestato dei mezzi di difesa»)[47]. Infine, così concepita la fattispecie non pare nemmeno idonea a ricomprendere tutti quei casi (sempre più frequenti, ma tuttora connotati da una controversa rilevanza penale[48]) nei quali l'*introduzione* e la *permanenza* negli altrui sistemi informatici avvengano *con il consenso* dell'avente diritto, mentre siano piuttosto le modalità *d'uso* di tali sistemi a violare le intenzioni del titolare: ipotesi che la giurisprudenza ha comunque sussunto nell'ambito applicativo dell'art. 615-*ter* c.p.[49], ma che se avvenissero nella realtà fisica presumibilmente non verrebbero ricondotte alla fattispecie di violazione di domicilio.

Proprio a causa delle descritte implicazioni che la metafora del *domicilio* produce rispetto all'interpretazione della fattispecie, è significativo osservare come, nell'applicazione giurisprudenziale, gli interpreti abbiano a tal punto avvertito l'esigenza di "forzare" la "gabbia" ermeneutica, derivante dall'immagine prescelta dal legislatore per rappresentare il sistema informatico, che attualmente la fattispecie di cui all'art. 615-*ter* c.p. finisca per trovare applicazione in casi piuttosto distanti dall'ispirazione originaria della disciplina, perché privi di un disvalore "di *intrusione*": ad esempio, per sanzionare l'eccesso o lo sviamento di potere del pubblico agente, che, per ragioni *diverse* dall'assolvimento dei compiti lui demandati, si introduca o si mantenga in un sistema informatico all'interno del quale è, tuttavia, abilitato a entrare e

[47] I virgolettati sono tutti ripresi da M. MELONI, *sub* Art. 615-ter - Accesso abusivo ad un sistema informatico o telematico, in M. RONCO, B. ROMANO (a cura di) *Codice penale commentato online*, Wolters Kluwer, 2022, reperibile su *wolterskluwer.it*. Come ricorda l'A., parte della dottrina ha anche ritenuto che «il requisito della protezione mediante misure di sicurezza abbia la sola funzione di denotare la volontà del titolare di negare l'accesso agli estranei».

[48] Cfr. ancora M. MELONI, *sub* Art. 615-ter - Accesso abusivo ad un sistema informatico o telematico, cit., nella parte relativa all'*utilizzazione abusiva di un accesso autorizzato*.

[49] Cfr. Cass. pen., SS. UU., 27 ottobre 2011, n. 4694, in *Cass. pen,* 2012, 11, 3681 ss., con nota di C. PECORELLA, che hanno affermato il principio di diritto secondo il quale «integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615-ter cod. pen., la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso».

mantenersi, in ragione della qualifica ricoperta[50]. Nuovamente, un'ipotesi che, se realizzata dal pubblico agente nella realtà fisica (ad esempio consultando un archivio cartaceo, anziché un archivio digitale), potrebbe assumere rilievo se ulteriormente corrispondente alla violazione di un dovere o di un segreto dell'ufficio, ma che non parrebbe – almeno a chi scrive – autonomamente rilevante (nel diritto penale), per il solo fatto dell'accesso.

Come denunciato da parte della dottrina, la volontà (se non la necessità) degli interpreti di sottrarsi ai vincoli ermeneutici derivanti dalla (talora controproducente) metafora del domicilio ha allora reso l'art. 615-*ter* c.p. una fattispecie dai confini piuttosto indefiniti, interpretata dalla giurisprudenza secondo cadenze che ormai prescindono dal testo normativo e che perciò possono dar vita a risvolti incompatibili con il principio di legalità penale[51].

4.2. - *Lo "strumento informatico o telematico" tra ampliamento semantico e mutamento fenomenico*

Si è già anticipato come – oltre alle implicazioni che la scelta di procedere "per metafore" ha avuto in relazione a singole figure incriminatrici – il disordinato inserimento dei reati informatici e cibernetici nelle maglie del codice «sulla base di presunte ma infondate analogie»[52] abbia avuto non trascurabili ripercussioni anche sulla comprensione del fenomeno del *cybercrime* nel suo complesso, cui è riconducibile una disciplina piuttosto disarticolata e talora priva di una coerenza sistematica.

[50] Cfr. in particolare Cass. pen., SS. UU., 18 maggio 2017, n. 41210, in *Ilpenalista.it*, 18 settembre 2017, con nota di C. PARODI. La sentenza afferma per l'appunto che: «Ad avviso del Collegio non esce dall'area di applicazione della norma la situazione nella quale l'accesso o il mantenimento nel sistema informatico dell'ufficio a cui è addetto il pubblico ufficiale o l'incaricato di pubblico servizio, seppur avvenuto a seguito di utilizzo di credenziali proprie dell'agente ed in assenza di ulteriori espressi divieti in ordine all'accesso ai dati, si connoti, tuttavia, dall'abuso delle proprie funzioni da parte dell'agente, rappresenti cioè uno sviamento di potere, un uso del potere in violazione dei doveri di fedeltà che ne devono indirizzare l'azione nell'assolvimento degli specifici compiti di natura pubblicistica a lui demandati».

[51] Cfr. ad es. S. SEMINARA, *Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente (art. 615-ter, c. 2, n. 1, c.p.)*, in *MediaLaws – Rivista dir. media*, 2018, n. 2, 235 ss. e in part. 249, nel senso che si tratta di «un'invenzione della giurisprudenza, che non trova nessun appiglio nel testo normativo – rivelandosi quindi incompatibile con il principio di legalità – e non appare dotata di un sufficiente fondamento politico-criminale».

[52] Si esprime in questi termini S. SEMINARA, *Codice penale, riserva di codice e riforma dei delitti contro la persona*, in *Rivista Italiana di Diritto e Procedura Penale*, 2, 2020, 421 ss.

A tale riguardo, sarà sufficiente osservare come, in una serie di disposizioni piuttosto eterogenee, l'intervento modificativo di "aggiornamento" del codice alla dimensione informatica sia stato congegnato con l'esclusivo fine di allargare legislativamente il *significato* di alcuni lemmi utilizzati all'interno di disposizioni incriminatrici: ad esempio, si è precisato, in alcune fattispecie, che le nozioni di "cose", "strumenti", "documenti", "mezzi" ricomprendano *anche* programmi, sistemi e documenti informatici, senza che, tuttavia, ciò abbia implicato alcuna modifica in punto di disciplina o di trattamento sanzionatorio[53]. Secondo un simile schema, ad esempio, nella sezione relativa ai *delitti contro la inviolabilità dei segreti* sono state introdotte le fattispecie di cui agli artt. 617-*quater* c.p. (*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*), 617-*quinquies* c.p. (*Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche*) e 617-*sexies* c.p. (*Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*), che riproducono specularmente le fattispecie e il trattamento sanzionatorio di cui agli artt. 617, 617-*bis*, 617-*ter* c.p. (relativi alle comunicazioni o conversazioni telegrafiche o telefoniche), estendendone semplicemente l'ambito applicativo anche a comunicazioni avvenute per il tramite di strumenti informatici e telematici.

In questi casi è, dunque, evidente che l'intervento legislativo rispondesse all'esclusivo intento di includere su un piano principalmente *semantico* i fenomeni

[53] Seguendo l'ordine del codice, un primo riferimento di questo tenore a programmi e sistemi informatici o telematici si rinviene nell'art. 392 c.p., relativo all'esercizio arbitrario delle proprie ragioni, ove al co. 3 si precisa che sussista altresì violenza sulle cose allorché un programma informatico venga alterato, modificato o cancellato in tutto o in parte ovvero venga impedito o turbato il funzionamento di un sistema informatico o telematico. Un analogo riferimento si rinviene, poi, nel successivo art. 461 c.p., ove in relazione alla fabbricazione o alla detenzione di strumenti destinati alla falsificazione di monete, si è avvertita l'esigenza di ricomprendervi espressamente anche «programmi e dati informatici» che siano destinati a tale scopo. Inoltre, in materia di falsità in atti, l'art. 491-*bis* stabilisce poi che tutte le falsità previste dal codice si applichino anche in relazione al *documento informatico pubblico* che abbia efficacia probatoria. Ancora, all'art. 493-*quater* c.p. i «programmi informatici» sono testualmente affiancati ad altre «apparecchiature» e altri «dispositivi» diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti. Un riferimento esplicito a dati e programmi informatici è rinvenibile altresì nell'art. 601-*bis* c.p., ove si precisa, con riguardo al traffico di organi prelevati da persona vivente, che sia incriminata la condotta di chiunque organizza o propaganda viaggi ovvero pubblicizza o diffonde, con qualsiasi mezzo annunci finalizzati al traffico di organi o parti di organi di cui al primo comma, «anche per via informatica o telematica». Infine, all'art. 616 c.p. si precisa che per «corrispondenza» deve intendersi anche quella «informatica o telematica», così come all'art. 621 c.p. in tema di rivelazione del contenuto di documenti segreti si specifica che sia «considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi».

informatici all'interno di una disciplina preesistente, che rimane però immutata nella sua configurazione.

In altre disposizioni, invece, l'estensione della nozione di "mezzo" anche allo strumento informatico o telematico non ha avuto mero valore *semantico*, ma ha prodotto conseguenze anche in termini di disciplina: in alcune ipotesi di reato, infatti, il riferimento all'«aver commesso il fatto mediante strumenti informatici o telematici» è stato introdotto dal legislatore non già al solo fine di specificare che anche un sistema informatico potesse costituire il "mezzo del reato", quanto invece per ricondurre a tale specifica forma di manifestazione l'applicazione di una circostanza aggravante speciale[54]. In tutte queste ipotesi, dunque, il riferimento esplicito a strumenti informatici e telematici sembra sottintendere che il legislatore ora ravvisi un rilevante mutamento *fenomenico*: a fronte della tutela del medesimo bene giuridico, sarebbe la diversa *modalità* di commissione del reato – e, in particolare, la maggiore offensività della condotta derivante dalla commissione di tale delitto mediante strumenti informatici e telematici[55] – a richiedere e giustificare il relativo aumento di pena.

È appena il caso di rilevare, tuttavia, come il discrimine tra il ricorso all'uno o all'altro modello risulti tutt'altro che definito: se, infatti, è comprensibile che in alcuni casi il *mezzo informatico* rappresenti soltanto un'alternativa modalità di esecuzione

[54] È il caso: del delitto di *Addestramento ad attività con finalità di terrorismo anche internazionale* di cui all'art. 270-*quinquies* c.p., ove si prevede che le pene sono aumentate se il fatto di chi addestra o istruisce è commesso attraverso strumenti informatici o telematici; del delitto di *Istigazione* a commettere alcuno dei delitti contro la personalità internazionale dello Stato o contro la personalità interna (art. 302 c.p.), ove si prevede analogamente che la pena sia aumentata in ragione della circostanza che il fatto sia commesso attraverso strumenti informatici o telematici; del delitto di *Istigazione a delinquere* di cui all'art. 414 c.p., ove nuovamente si prevede che la pena sia aumentata se il fatto è commesso attraverso strumenti informatici o telematici (co. 3 e 4); del delitto di *Atti persecutori* (art. 612-*bis*, co. 2, c.p.), rispetto al quale la pena è aumentata se il fatto è commesso attraverso strumenti informatici o telematici; del delitto di *Diffusione illecita di immagini o video sessualmente espliciti* (art. 612-*ter* c.p.), la cui pena è aumentata se i fatti sono commessi attraverso strumenti informatici o telematici; infine, è il caso del delitto di *Rivelazione di segreti scientifici e commerciali* di cui all'art. 623 c.p., ove si dispone che se il fatto relativo ai segreti commerciali è commesso tramite qualsiasi strumento informatico la pena è aumentata. Similmente, all'art. 602-*ter* c.p. si prevede che per i delitti contro la personalità individuale che vi sono elencati, le pene siano aumentate, in misura non eccedente i due terzi, nei casi in cui gli stessi siano compiuti con l'utilizzo di mezzi atti ad impedire l'identificazione dei dati di accesso alle reti telematiche.

[55] In tal senso, cfr. ad es. Cass. pen., sez. V, 28 ottobre 2022, n. 44214, non massimata, reperibile su banca dati *Dejure*, osserva come, con riferimento al delitto previsto dall'art. 612-*bis* c.p., l'utilizzo di «strumenti informatici o telematici», com'è anche previsto per l'uso di armi, debba essere «riguardato come momento di caratterizzazione di alcuni dei profili della condotta abituale, che il legislatore assume, rispetto all'offesa tipica, come espressivo di maggiore disvalore».

che tuttavia non implica una maggiore gravità del fatto (ad es. nelle fattispecie che puniscono condotte di *produzione*, nelle quali lo strumento informatico può essere equivalente ad altri mezzi), mentre in altri casi esso presenti un *peculiare* e *maggiore* disvalore (ad es. nelle fattispecie che puniscono condotte di *divulgazione* o *comunicazione* di contenuti o immagini, che hanno nella rete una più ampia diffusività), non può non rilevarsi, ad esempio, che nel delitto di «*Istigazione a delinquere*» di cui all'art. 414 c.p., la pena è aumentata se il fatto è commesso attraverso strumenti informatici o telematici, mentre nel successivo delitto «*Istigazione a pratiche di pedofilia e di pedopornografia*» di cui all'art. 414-*bis* c.p., il fatto è punito con la medesima pena ove commesso «con qualsiasi mezzo e con qualsiasi forma di espressione». Una simile differenza appare, almeno a prima vista, difficilmente spiegabile e sembra anzi il sintomo della già lamentata mancanza di una visione unitaria in questo settore.

Analoghe asimmetrie punitive si riscontrano, del resto, anche comparando i due ambiti dell'accesso abusivo e del danneggiamento di sistemi informatici: in sintesi, mentre nei primi il legislatore ha ritenuto la violazione del domicilio "informatico" meno grave rispetto alla violazione del domicilio "fisico" – e, dunque, pur ricalcando la forma delle incriminazioni, ha tuttavia previsto un trattamento sanzionatorio più lieve –, nel secondo caso il legislatore ha introdotto le fattispecie speciali di cui agli artt. 635-*bis* c.p. (*Danneggiamento di informazioni, dati e programmi informatici*), 635-*ter* c.p. (*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*), 635-*quater* c.p. (*Danneggiamento di sistemi informatici o telematici*), 635-*quinquies* c.p. (*Danneggiamento di sistemi informatici o telematici di pubblica utilità*), riprendendo la fattispecie generale di danneggiamento di cui all'art. 635 c.p. ma prevedendo un trattamento sanzionatorio tendenzialmente più severo (con la sola eccezione dell'art. 635-*bis* c.p.).

All'esito dell'analisi condotta sinora, occorre, dunque, dare atto della sostanziale «impossibilità di un inquadramento concettuale dei reati informatici»[56] nell'ordinamento italiano: com'è stato osservato, una definizione che si fondi su «un collegamento di qualsivoglia tipo con l'elaboratore elettronico» – o che utilizzi, quale criterio di selezione dei reati rilevanti, la sola constatazione delle «potenzialità criminogene di internet»[57] – finisce per l'essere «priva di ogni valore euristico e delimitativo»[58].

[56] Cfr. S. SEMINARA, *Internet (dir. pen.)*, cit., 568.

[57] Cfr. ancora S. SEMINARA, *Internet (dir. pen.)*, cit., 568.

[58] Cfr. C. PECORELLA, *Il diritto penale dell'informatica*, cit., 3.

Se ciò costituisce conclusione invero piuttosto consolidata, si può tuttavia ora ipotizzare, alla luce dell'interpretazione proposta, che essa dipenda anche dalla scelta di disciplinarne le diverse possibili manifestazioni, come si è visto, ricorrendo a (rassicuranti) analogie rispetto a modelli di incriminazione e aree di tutela già collaudati: ciò ha, infatti, talora impedito un'effettiva e sostanziale comprensione della realtà di cui si tratta, soprattutto laddove l'immagine metaforica abbia "represso" o, comunque, non adeguatamente valorizzato i tratti essenziali di un nuovo fenomeno criminoso. Ad ogni modo, la presenza di (soltanto) *alcune* e *specifiche* disposizioni penali dedicate al fenomeno della criminalità informatica – peraltro con esiti che, all'interno di questo sottosistema normativo, risultano talora *distonici* – induce a porre in dubbio la coerenza del sistema nel suo complesso con i principi delineati dall'art. 3 della Costituzione e, in particolare, con l'esigenza di disciplinare in modo *uguale* casi *uguali* e in modo *diverso* casi *diversi*.

4.3. - *La specialità dei soli rimedi: l'esempio (virtuoso) del cyberbullismo*

Un approccio sensibilmente diverso al fenomeno del *cybercrime* è invece rinvenibile nella recente l. 71/2017, dedicata al c.d. *cyberbullismo*. Il tratto d'interesse di tale intervento normativo si rinviene, ad avviso di scrive, nella peculiare tecnica legislativa utilizzata: in questo caso, infatti, il legislatore non ha mediato la costruzione giuridica del fenomeno ricorrendo a (suggestive quanto potenzialmente fuorvianti) metafore, ma ha guardato direttamente alla *sostanza* del fenomeno, predisponendo appositi strumenti di tutela e di contrasto rispetto a un fenomeno accompagnato da un sempre maggiore allarme sociale[59].

Invero, valorizzando, anche sulla scorta di studi di carattere psicologico e sociologico, le peculiarità *criminologiche* di tale fenomeno[60], il legislatore ha tuttavia ritenuto

[59] Cfr. M. C. PARMIGGIANI, *Il* cyberbullismo, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), *Trattato di diritto penale – Cybercrime*, Milano, UTET, 2019, 631 ss.; C. GRANDI, *Il "reato che non c'è": le finalità preventive della legge n. 71 del 2017 e la rilevanza penale del cyberbullismo*, in *Studium Iuris*, 2017, 12, 1440 ss.

[60] Com'è riportato nel *Dossier* relativo a «*Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del bullismo e del cyberbullismo*», reperibile sul sito *documenti.camera.it*, «secondo un inquadramento di tipo psicologico, gli studiosi hanno complessivamente ricostruito le seguenti categorie di cyberbullismo: - *flaming*: messaggi on line violenti e volgari mirati a suscitare battaglie verbali in un forum; - molestie (*harassment*): spedizione ripetuta di messaggi insultanti mirati a ferire qualcuno; denigrazione: sparlare di qualcuno per danneggiare gratuitamente e con cattiveria la sua reputazione, via e-mail, messaggistica istantanea, gruppi su *social network*, ecc.; - sostituzione di

di non dover introdurre alcuna *nuova* disposizione penale, piuttosto riconoscendo che – a seconda delle concrete modalità esecutive, che dovranno essere di volta in volta considerate – il *cyberbullismo* possa alternativamente costituire «una forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo»[61], ciascuna connotata da una (eventuale) autonoma e specifica rilevanza penale.

L'elemento di *novità* che caratterizza la strategia di contrasto al *cyberbullismo* è invece rappresentato dalla scelta di intervenire sul versante dei *rimedi*: come si anticipava, infatti, proprio alla luce delle peculiarità del fenomeno, il legislatore ha introdotto nella l. 71/2017 appositi strumenti *extra-penali (preventivi* e *successivi*; *cautelari* e *ripristinatori*), prevedendo, da un lato, interventi a carattere «formativo, educativo e divulgativo», in un'ottica di «prevenzione generale sociale»[62], e, dall'altro lato, strumenti per l'immediato ed efficace oscuramento, blocco o rimozione dei contenuti illeciti eventualmente diffusi ai danni di minori nella rete internet[63]. La risposta ideata

persona (*impersonation*): farsi passare per un'altra persona per spedire messaggi o pubblicare testi reprensibili; - rivelazioni (*exposure*): pubblicare informazioni private o imbarazzanti su un'altra persona; inganno; - (*trickery*): ottenere la fiducia di qualcuno con l'inganno per poi pubblicare o condividere con altri le informazioni confidate via mezzi elettronici; esclusione: escludere deliberatamente una persona da un gruppo on line per provocare in essa un sentimento di emarginazione; - cyber persecuzione (*cyberstalking*): molestie e denigrazioni ripetute e minacciose mirate a incutere paura». Inoltre, come si osserva, «rispetto al bullismo tradizionale, l'uso dei mezzi elettronici conferisce al cyberbullismo alcune caratteristiche proprie quali: - *l'anonimato del molestatore* […]; - *la difficile reperibilità*; […]; - *l'indebolimento delle remore etiche*; - *l'assenza di limiti spazio-temporali*».

[61] Cfr. art. 1 l. 71/2017 «Finalità e definizioni».

[62] C. GRANDI, *Il "reato che non c'è": le finalità preventive della legge n. 71 del 2017 e la rilevanza penale del cyberbullismo*, cit., 1441.

[63] In argomento cfr. ancora C. GRANDI, *Il "reato che non c'è": le finalità preventive della legge n. 71 del 2017 e la rilevanza penale del cyberbullismo*, cit., 1441 ss. Rientrano nell'ambito dei rimedi di carattere preventivo quelli di cui agli artt. 3 («Piano di azione integrato»), 4 («Linee di orientamento per la *prevenzione* e il contrasto in ambito scolastico») e 6 (in materia di oneri informativi della Polizia postale e finanziamento delle attività di formazione); ha, invece, natura eminentemente cautelare-ripristinatoria quanto previsto dall'art. 2, che attribuisce al minore e ai genitori la facoltà di richiedere «inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete internet», anche laddove le condotte non integrino gli estremi di una fattispecie tra quelle indicate all'art. 1, nonché la facoltà di rivolgere un'analoga richiesta al Garante per la protezione dei dati personali, qualora il destinatario della prima istanza non fosse identificabile o, comunque, non abbia

dal legislatore risulta dunque mirata, grazie a una precisa messa a fuoco dell'oggetto della disciplina.

Prescindendo da più ampie considerazioni in ordine alle specificità di tale intervento normativo – che ovviamente esulano dall'oggetto della presente analisi –, ciò che interessa sottolineare è, dunque, la peculiare *forma* di tale intervento normativo, che, non costringendo il fenomeno del *cyberbullismo* entro un'angusta etichetta metaforica, ha determinato l'introduzione di una disciplina (non solo *speciale*, ma anche e soprattutto) *specifica*, che si confronta direttamente con le caratteristiche e le peculiarità *sostanziali* del fenomeno criminoso regolato.

5. La criminalità informatica nell'interpretazione della giurisprudenza di legittimità: usi e abusi del linguaggio metaforico

Proseguendo nel percorso delineato in premessa, si esaminerà ora l'attitudine interpretativa che si registra invece nella giurisprudenza penale, quando si tratti di decidere di casi che a vario modo si collochino nell'ambiente digitale. Lo scopo è, per l'appunto, quello di verificare empiricamente se, come e con quali conseguenze i giudici applichino "per similitudine" il diritto penale tradizionale al cyberspazio: scomponendo, dunque, il ragionamento giudiziale, ci si concentrerà nello specifico sulle strategie argomentative utilizzate, con l'obiettivo di capire a quali intenti esse rispondano e quali effetti esse producano, rispetto al fenomeno criminoso in questione.

In termini generali, la stessa Corte di Cassazione ha riconosciuto come la diffusione di *internet* e, quindi, «l'aumento esponenziale delle occasioni di connessione e condivisione in rete» pongano il sostanziale problema «della previsione normativa di fattispecie che prevedano un sistema sanzionatorio finalizzato ad arginare il fenomeno della graduale crescita degli illeciti commessi dagli internauti»[64]; invero, come ancora osserva la Suprema Corte, «la casistica di illeciti è variegata e, in ragione della iperbolica amplificazione del sistema, crea *forti problematiche di tipizzazione*, con riguardo ai numerosi fenomeni che caratterizzano l'uso illecito del web»[65]. Il problema metodologico-definitorio risulta, dunque, precisamente avvertito dalla Corte di Cassazione,

rapidamente provveduto alla rimozione; infine, l'art. 5 prevede espressamente che le condotte di cyberbullismo debbano costituire infrazioni disciplinari nell'ordinamento scolastico.

[64] Cfr. Cass. pen., sez. V, 12 aprile 2019, n. 30737, non massimata, reperibile su banca dati *Dejure*.

[65] Cfr. Cass. pen., sez. V, 8 novembre 2018, n. 12546, in *Guida al diritto*, 2019, 20, 84, corsivo aggiunto.

che colloca sul piano della *tipicità* – e, dunque, della riconducibilità del *fatto* alla *disposizione* – piuttosto che su quello della *comprensione-descrizione del fatto*, la questione essenziale da sciogliere, nel rapporto tra diritto e fenomeno tecnologico.

Ebbene, una serie di casi che saranno riportati di seguito dimostra come, anche nell'applicazione giurisprudenziale, si rinvengano esempi del ricorso a un pensiero metaforico al fine di guidare (o talvolta fuorviare) la descrizione dei fenomeni che si verificano nel *cyberspazio* e di individuare, di conseguenza, la disciplina applicabile; in parallelo, si vedrà tuttavia come in altri casi si registri un'opposta tendenza a negare l'*assimilazione* tra realtà fisica e realtà virtuale, per escludere (ora *in bonam partem,* ora anche *in malam partem*) l'estensione della disciplina esistente.

A riprova di tale ultima tendenza, è possibile citare sin d'ora l'esempio del sequestro dell'*e-mail*, utilizzato dalla dottrina citata in premessa quale "cartina di tornasole" per verificare l'attitudine interpretativa della giurisprudenza di fronte a nuovi fenomeni di carattere tecnologico: e ciò sul presupposto per cui, quando si tratti di valutare quale sia la disciplina applicabile all'acquisizione di una *e-mail* nell'ambito di un'indagine, il problema della prospettiva da adottare si rivela essenziale. Nello specifico, infatti, mentre da una prospettiva interna la *e-mail* inviata o ricevuta dall'utente può farsi corrispondere funzionalmente alla (ormai datata) corrispondenza postale, da una prospettiva esterna la comunicazione *e-mail* si riduce, invece, a un flusso di dati, al contenuto informatico accessibile dal pc dell'utente, ma conservato anche sui *server* del fornitore di servizi di posta elettronica[66].

Si tratta di una distinzione di non secondario rilievo, dato che, a seconda che si adotti l'una o l'altra prospettiva, potrebbe risultare o meno applicabile la tutela "rafforzata" che l'art. 15 Cost. assicura alla libertà e alla segretezza della corrispondenza (declinata anche nel codice di rito dall'art. 254 c.p.p.). Ebbene, la Corte di Cassazione propende, nell'ordinamento interno, per la seconda impostazione interpretativa, ritenendo che «i messaggi di posta elettronica memorizzati nelle cartelle dell'account o nel computer del mittente ovvero del destinatario, costituiscono *meri documenti informatici* intesi in senso "statico"» e, dunque, siano normalmente acquisibili ai sensi dell'art. 234 c.p.p.[67]. Come osserva condivisibilmente la Corte, in effetti la questione interpretativa non si risolve nell'equiparazione tra *corrispondenza cartacea* e *corrispondenza digitale*, ma impone piuttosto di distinguere tra corrispondenza *in atto* (quella prevista dall'art. 254 c.p.p., che appunto si applica presso coloro che forniscono

[66] Cfr. O. KERR, *The Problem of Perspective in Internet Law*, cit., 365 ss.

[67] Cfr. Cass. pen., sez. VI, 6 febbraio 2020, n.12975, in *CED Cass. 2020* rv. 278808, corsivi aggiunti.

servizi postali, telegrafici, telematici o di telecomunicazioni, ove si trovi la corrispondenza *spedita* da o verso l'indagato/imputato, ma non *consegnata*) e documenti invece «frutto di una dinamica comunicativa già avvenuta»[68]. In questo specifico caso, dunque, la giurisprudenza sembra rifuggire da una similitudine nominalistica – quella tra *e-mail* e corrispondenza – che a prima vista poteva apparire scontata, valorizzando le specifiche modalità di funzionamento di tale forma di comunicazione elettronica. Un simile approccio può risultare condivisibile a condizione, beninteso, che la disciplina di cui all'art. 254 c.p.p. venga invece applicata qualora, ad esempio, si proceda al sequestro *presso il provider*, oppure qualora – com'è stato ipotizzato – l'attiva acquisitiva abbia ad oggetto «messaggi pervenuti in tempo reale, all'insaputa del destinatario»[69] e, dunque, la dinamica comunicativa non si sia ancora esaurita.

5.1. - *Alcune strategie argomentative per ancorare il* Web *alla realtà fisica*

Volendo fornire ulteriori esempi dell'attitudine interpretativa che si riscontra nella giurisprudenza di legittimità, è possibile operare un primo riferimento ad alcune pronunce, nelle quali la Corte di Cassazione rivolge ai giudici di merito un monito a non lasciarsi ingannare dall'apparente dematerializzazione e delocalizzazione dei contenuti pubblicati in rete – che deriverebbe dalla natura "ubiquitaria", "circolare" e "diffusa" del Web[70] – e a concentrarsi, invece, sulla dimensione "fisica" di ciascuno dei fenomeni considerati. In questo ambito, la giurisprudenza sembra allora ripudiare quelle metafore – *in primis* quella di "*cyberspazio*" – che enfatizzano la novità e l'apparente inconsistenza materiale della rete e dei programmi informatici.

Questa impostazione si rinviene, ad esempio, in una fondamentale sentenza della Suprema Corte, relativa alla collocazione *spaziale* della condotta criminosa realizzata nel contesto digitale[71]: in tale pronuncia, infatti, la Corte osserva come «la condotta illecita commessa in un ambiente informatico o telematico assuma delle

[68] Cfr. Cass. pen., sez. III, 16 aprile 2019, n. 29426, in *Guida al diritto*, 2019, 38, 102 ss. In relazione alla rilevanza di questo tema e all'inclusione della *mail* nella nozione di corrispondenza, *cfr.* ad es. M. MINAFRA, *Prove e messaggi telematici remoti: sul giusto metodo acquisitivo della corrispondenza informatica "statica"*, in *Giur. It.,* 2018, 7, 1718 ss.

[69] Cfr. in termini G. ILLUMINATI, *Libertà e segretezza della comunicazione,* in *Cass. pen.*, 2019, 11, 3826 ss. e in part. 3827.

[70] Cfr. in termini Cass. pen., sez. un., 24 aprile 2015, n. 17325, in *Dir. e Giust.*, 2015, 18, 65 ss., con nota di F. CAPITANI, *Il reato informatico si verifica nel luogo dell'accesso abusivo e non in quello di ubicazione del server* e in *Cass. pen.*, 2015, 10, 3507 ss., con nota di M. L. SCIUBA.

[71] Cfr. ancora Cass. pen., sez. un., 24 aprile 2015, n. 17325, cit.

specifiche peculiarità per cui la tradizionale nozione – elaborata per una realtà fisica nella quale le conseguenze sono percepibili e verificabili con immediatezza – deve essere rivisitata e adeguata alla dimensione virtuale», rilevando come «nel *cyberspace* i criteri tradizionali per collocare le condotte umane nel tempo e nello spazio entrano in crisi, in quanto viene in considerazione una dimensione "smaterializzata" (dei dati e delle informazioni raccolti e scambiati in un contesto virtuale senza contatto diretto o intervento fisico su di essi) ed una complessiva "delocalizzazione" delle risorse e dei contenuti (situabili in una sorta di meta-territorio)»[72].

Al netto di tali premesse, tuttavia, la Corte ritiene che, in questo scenario, la materialità della condotta possa (e debba) essere, comunque, recuperata con il riferimento all'atto fisico della "digitazione" da parte del soggetto attivo, la quale effettivamente rappresenterebbe «l'unica condotta umana di natura materiale». Con un approccio, dunque, programmaticamente «coerente con la realtà di una rete telematica», la Suprema Corte adotta una prospettiva marcatamente *esterna*, valorizzando la (sola) dimensione *fisica* della rete, anche al fine di potervi applicare la legislazione rilevante[73] e conclude conseguentemente – nel caso di specie – che il luogo di consumazione del delitto di cui all'art. 615-*ter* c.p. «è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente». Con l'effetto per certi versi paradossale – se si ripensa a quanto prima osservato – che la violazione del domicilio informatico (della persona offesa) si consuma (con tutte le implicazioni che ne derivano) presso il domicilio dell'autore del fatto.

Un'impostazione per certi versi analoga si rinviene inoltre in altre ben note pronunce, nelle quali la Corte di Cassazione è stata chiamata a valutare se i dati memorizzati in un *computer* possano costituire una "cosa mobile", suscettibile di furto, appropriazione indebita, ricettazione. Come si è visto, infatti, in alcuni casi – come nell'ipotesi di cui all'art. 392 c.p., ove è specificato che sia abbia violenza sulle «cose» anche allorché un programma informatico venga alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico – il legislatore è intervenuto espressamente a specificare che anche dati, programmi e informazioni rientrassero nella nozione di «cosa», evidentemente ritenendola un'assimilazione altrimenti problematica sul piano meramente interpretativo[74].

[72] Così Cass. pen., sez. II, 29 settembre 2016, n. 43705, in *Riv. pen.* 2016, 12, 1104.

[73] Cfr. ancora in termini Cfr. Cass. pen., sez. un., 24 aprile 2015, n. 17325, cit.

[74] Come si osservava nella Relazione del Disegno di legge n. 2773, cit., «del resto, la sottrazione di

Ebbene, la Corte di Cassazione – ritenendo di non poter estendere *tout court* la nozione di «cosa mobile» fino a ricomprendervi anche dati e programmi informatici, ma considerata altresì l'esigenza di non lasciare impunite condotte che dovevano evidentemente apparire meritevoli di pena e del tutto paragonabili ad analoghe condotte realizzate nella realtà fisica – ha operato una sorta di "equilibrismo" interpretativo, applicando la relativa fattispecie incriminatrice rilevante – nel caso di specie, la ricettazione, il cui oggetto è costituito da «denaro o cose» – e al contempo precisando che la "cosa mobile" non dovesse individuarsi nel "dato", ma più semplicemente nel supporto informatico *hardware* nel quale tali dati erano stati trasferiti[75]. Con l'effetto, tuttavia, di condizionare la punibilità di una determinata condotta (ad es. la sottrazione di dati e il trasferimento di questi a terzi, a fini di profitto) alla sola quanto accidentale (e irrilevante, rispetto al disvalore del fatto) evenienza che tali *file* vengano o meno archiviati in un supporto materiale.

Nella medesima direzione, la Corte di Cassazione ha ritenuto configurabile il delitto di appropriazione indebita rispetto alla condotta di colui che, accedendo abusivamente a un sistema informatico, si procurava i dati bancari di una società riproducendoli su un supporto cartaceo, sul presupposto che, sebbene «il dato bancario» costituisca bene immateriale insuscettibile di detenzione fisica, è «invece cosa mobile l'entità materiale su cui beni immateriali vengono trasfusi» e che pertanto acquisisce il valore di questi[76]. Nuovamente, un simile approccio interpretativo pare eccessivamente condizionato da una prospettiva *esterna*, che valorizzando all'estremo la dimensione "*tangibile*" del fenomeno tecnologico, forse ne sopravvaluta la differenza (solo esteriore e *materiale*) rispetto all'equivalente *fisico* e così ne preclude una comprensione sostanziale e funzionale: come si è già anticipato, infatti, può risultare ingiustificato che la tutela penale del *file* dipenda dalla sua eventuale incorporazione o stampa su un supporto fisico, piuttosto che – ad esempio – dal suo valore economico, o più in generale dal suo contenuto.

dati, quando non si estenda ai supporti materiali su cui i dati sono impressi (nel qual caso si configura con evidenza il reato di furto), altro non è che una «presa di conoscenza» di notizie, ossia un fatto intellettivo rientrante, se del caso, nelle previsioni concernenti la violazione dei segreti. Ciò, ovviamente, a parte la punibilità ad altro titolo delle condotte strumentali, quali ad esempio, quelle di violazione di domicilio (art. 614 c.p.), eccetera».

[75] Cass. pen., sez. II, 18 febbraio 2016, n. 21596, su *Ilpenalista.it*, 22 giugno 2016, con nota di M. TRAPASSO.

[76] Cass. pen., sez. V, 30 settembre, 2014, n. 47105, in *Riv. pen.*, 2015, 1, 34 ss.

Soltanto più di recente la Corte di Cassazione è fuoriuscita da tale "finzione" interpretativa riconoscendo di dover considerare in modo nuovo quelle «categorie giuridiche […] coniate in epoche in cui erano del tutto sconosciute le attuali tecnologie informatiche», anche al fine di «render effettiva la tutela cui mirano le disposizioni incriminatrici dei delitti contro il patrimonio»[77]. Si legge, allora, nella sentenza citata – dopo un'approfondita disamina della nozione *tecnica* di *file* – che, «indiscusso il valore patrimoniale che il dato informatico possiede» (potendo esso, al pari della cosa mobile *materiale*, essere oggetto di condotte di sottrazione, di impossessamento, di utilizzazione), la «limitazione che deriverebbe dal difetto del requisito della "fisicità" della detenzione», per come tradizionalmente intesa, non costituirebbe «elemento in grado di ostacolare la riconducibilità del dato informatico alla categoria della cosa mobile».

Ciò che preme sottolineare è come la Corte spenda un argomento che, ad avviso di chi scrive, è convincente e centrato, in quanto induce a liberare il *web* da una sorta di "presunzione di novità" che non è mai stata, per converso, così marcata, con riguardo ad altre innovazioni della realtà materiale: la sentenza cita, al riguardo, l'esempio del *denaro*, rispetto al quale si porrebbero – quanto al requisito della *fisicità* – «le medesime questioni sollevate in relazione ai dati informatici», atteso che il denaro, pur essendo in alcuni casi «fisicamente suscettibile di diretta apprensione materiale», è ovviamente «suscettibile di operazioni contabili, così come di trasferimenti giuridicamente efficaci, anche in assenza di una materiale apprensione delle unità fisiche» (le banconote, o le monete)[78].

In un altro caso, infine, dovendo valutare se anche una banca dati potesse ricondursi alla nozione di "cosa mobile" di cui all'art. 314 c.p., la Suprema Corte ha dato alla questione una soluzione affermativa, sul presupposto che appunto possano farsi rientrare nella nozione di *cosa mobile* oggetto di peculato «anche i beni c.d. immateriali tutte le volte in cui gli stessi abbiano un diretto ed intrinseco valore economicamente apprezzabile»[79].

Questo più recente mutamento di prospettiva – funzionale a ricomprendere il *file* nella nozione di "cosa" in virtù delle sue caratteristiche intrinseche e non già mediante il riferimento al supporto *hardware* nel quale il dato è archiviato – pare il più convincente, dal momento che esso considera il *file* per ciò che è, e non per ciò che metaforicamente appare o per ciò che lo incorpora.

[77] Cfr. Cass. pen., sez. II, 7 novembre 2019, n. 11959, in *Guida al diritto*, 2020, 34-35, 84 ss.

[78] Cfr. ancora Cass. pen., sez. II, 7 novembre 2019, n. 11959, cit.

[79] Cass. pen., sez. VI, 9 maggio 2018, n. 33031, in *CED Cass. 2018* rv. 273775.

5.2. - *Internet come "luogo pubblico" e come "luogo abbandonato e isolato"*

In un'opposta prospettiva – parimenti significativa nell'ambito della presente analisi – si collocano, invece, altre pronunce nelle quali la Corte di cassazione fa espresso ricorso a un linguaggio metaforico per inquadrare il fenomeno tecnologico: tra queste, si prenderanno in considerazione alcune sentenze nelle quali la Suprema Corte ha esplicitamente affermato che *Facebook* e i *social network* debbano essere considerati come una "piazza virtuale" e perciò possano essere qualificati come un "luogo pubblico" ai fini dell'applicazione della legge penale.

In tal senso, al fine di determinare la disciplina applicabile a condotte – ad es. di molestie o diffamazione – poste in essere *online*, la Corte di Cassazione ha, ad esempio, affermato che una bacheca telematica, in quanto « area di discussione, in cui qualsiasi utente o i soli utenti registrati (forum chiuso) sono liberi di esprimere il proprio pensiero, rendendolo visionabile agli altri soggetti autorizzati ad accedervi» – possa essere concepita come una "piazza" virtuale, nella quale avviene un libero confronto di idee[80]. Diversamente, se il forum è una «piazza virtuale», il blog è invece da considerarsi soltanto «un'agenda personale aperta e presente in rete»[81].

A fronte di tale orientamento, ciò che si vuole evidenziare è come tali metafore (non sempre calzanti) non abbiano un significato soltanto "evocativo", ma producano consistenti implicazioni pratiche: ad esempio, proprio la definizione di *Facebook* quale «agorà virtuale» e «piazza immateriale» ha consentito alla Corte di Cassazione di argomentare l'applicabilità dell'art. 660 c.p. – che punisce le molestie soltanto laddove queste avvengano in un *luogo pubblico* – anche a condotte di molestia poste in essere per il tramite del *social network*[82]. Le implicazioni di tale impostazione si rinvengono, del resto, anche *in negativo*, perché alla decisione di configurare le piattaforme come «luoghi» (pubblici e aperti) ai fini della legge penale corrisponde la correlativa decisione di negare che tali strumenti possano essere ricondotti – quanto alla tutela (costituzionale), ma anche alle connesse responsabilità – alla diversa nozione di «stampa», come si vedrà più avanti.

[80] Cass. pen., sez. V, 18 gennaio 2021, n. 8898, in *Dir. giust.*, 4 marzo 2021; Cass. pen., sez. V, 19 febbraio 2018, n. 16751, in *Cass. pen.*, 2018, 11, 3743 ss., con nota di PEDULLÀ.

[81] Cass. pen., sez. un., 29 gennaio 2015, n. 31022, in *Cass. pen.*, 2015, 10, 3437 ss., con nota di L. PAOLONI.

[82] Cass. pen., sez. I, 11 luglio 2014, n. 37596. Cfr. in proposito G. CHECCACCI, *Facebook come un luogo pubblico: un caso di "analogia digitale"* in malam partem, in *Criminalia*, 2014, 503 ss.

Per un certo verso assimilabile a tale approccio interpretativo pare, inoltre, un secondo filone giurisprudenziale, nell'ambito del quale la Corte di Cassazione ha più volte assimilato internet – per così dire – a un luogo buio e isolato, rilevando come la commissione di un illecito sul web consenta all'autore del reato di avvalersi dell'invisibilità e dell'anonimato che la rete gli garantisce, rendendo, dunque, ogni crimine più ingannevole e insidioso. È piuttosto recente, infatti, la pronuncia[83] nella quale la Corte di Cassazione ha stabilito che la perpetrazione del delitto di truffa *online* comporti l'applicazione dell'aggravante di cui all'art. 61, n. 5 c.p., ovverosia la c.d. minorata difesa caratterizzata nello specifico dall'approfittamento delle circostanze di luogo, tali da ostacolare la pubblica o privata difesa.

Si legge, infatti, nella citata pronuncia che – proprio come accade in un «luogo abbandonato o isolato […] distante da collegamenti con centri abitati, vie di comunicazione, presenze umane, tanto da indebolire la reazione pubblica o privata rispetto alla condotta illecita» – così anche nel *web* «la distanza tra il luogo di commissione del reato, ove l'agente si trova ed il luogo ove si trova l'acquirente del prodotto on line» sarebbe l'elemento che «consente all'autore della truffa di porsi in una posizione di maggior favore rispetto alla vittima, di schermare la sua identità, di fuggire comodamente, di non sottoporre il prodotto venduto ad alcun efficace controllo preventivo da parte dell'acquirente; tutti vantaggi che non potrebbe sfruttare a suo favore, con altrettanta comodità, se la vendita avvenisse *de visu*»[84].

Ebbene, anche tale equiparazione non pare del tutto convincente, non soltanto perché – come pure rilevato in altra pronuncia – essa finisce per attribuire «carattere "circostanziato" ad una delle possibili modalità della condotta di truffa», postulandosi per converso la prova – in ogni caso – «del concreto e consapevole approfittamento, da parte del colpevole, delle opportunità decettive offerte dalla rete»[85]; ma anche perché appare forse eccessivamente tributaria dell'immagine di internet come un "*Far web"* (non risulta, infatti, che la circostanza aggravante in parola sia richiamata per le ipotesi di vendita per corrispondenza che *non* avvengano nel *web*, pur essendo analoga la *distanza* tra venditore e acquirente). Peraltro, come segnalato dalla giurisprudenza di

[83] Così Cass. pen., sez. II, 29 settembre 2016, n. 43705, in *Riv. pen.* 2016, 12, 1104, nonché analogamente Cass. pen., sez. II, 14 gennaio 2021, n. 12427, in *Guida al diritto*, 2021, 15; Cass. pen., sez. VI, 22 marzo 2017, n. 17937, in *Foro it.*, 2017, 10, II, 576 ss.

[84] Cfr. ancora Cass. pen., sez. II, 29 settembre 2016, n. 43705, cit.

[85] Cass. pen., sez. II, 17 luglio 2018, n. 40045, cit., ove appunto si rileva l'impossibilità di escludere che «nel singolo caso la truffa sia realizzata bensì con lo strumento on line, ma senza che ciò comporti una reale, specifica situazione di vantaggio per l'autore».

merito, con approccio sicuramente più pragmatico, nel caso di trattativa *online* l'acquirente, «proprio in virtù dell'impossibilità di accertare, tramite una visione diretta, l'esistenza del bene offerto», è non soltanto «in grado di valutare – alla stregua della media diligenza – come rischiosa l'operazione», ma anche di cautelarsi da possibili frodi, ad esempio preferendo il pagamento alla consegna oppure optando per un sistema di pagamento che garantisca il rimborso in caso di inadempimento della controparte[86].

In entrambi i casi analizzati – quello della *piazza virtuale* e quello del *luogo isolato* – il ricorso a un linguaggio sostanzialmente metaforico ha, con tutta evidenza, lo scopo di argomentare l'applicazione di disposizioni incriminatrici – nello specifico, una fattispecie a sé stante e una circostanza aggravante – in modo decisamente creativo, rendendo così piuttosto indistinto il confine (e il rapporto) tra l'immagine e la realtà.

5.3. - *Le nozioni di "stampa" e "giornale" alla prova delle comunicazioni elettroniche*

Un ulteriore esempio, funzionale a valutare il ricorso a un'argomentazione "figurativa" nell'ambito del diritto penale dell'informatica, può essere tratto da una serie di pronunce, relative alla qualificazione *ai fini dell'applicazione della legge penale* delle diverse forme di comunicazione elettronica che si sono diffuse nella prassi. Anche in questo campo, infatti, la dottrina nordamericana richiamata in premessa aveva sottolineato come la «scelta della giusta metafora» costituisca un passaggio cruciale per determinare la disciplina applicabile alle nuove forme di comunicazione rese possibili da internet: sensibilmente diversi sono, infatti, gli esiti, a seconda che il gestore di una piattaforma digitale venga qualificato come un "editore", come un "distributore" o ancora come un mero "vettore", rispetto ai contenuti pubblicati sul portale[87].

Sul punto, si può allora innanzitutto richiamare quanto affermato dalle Sezioni Unite della Corte di Cassazione in relazione alla possibilità di sottoporre a sequestro preventivo una testata giornalistica *on line* regolarmente registrata o di una determinata pagina web di detta testata[88]. Invero, l'intervento delle Sezioni Unite era stato

[86] In tal senso, cfr. Trib. Pescara, 11 aprile 2022, n.912, reperibile su banca dati *Dejure*.

[87] In questo senso cfr. in particolare D. R. JOHNSON, K. A. MARKS, *Mapping Electronic Data Communications onto Exisiting Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide*, in *Villanova Law Review*, 1993, 38, 487 ss., e in part. 491: «*Few standards exist that can assist in determining who has what responsibility for harms caused by the contents of particular electronic messages or publications. We can, however, look broadly to three particularly relevant models: (1) publishers, (2) distributors and (3) common carriers*».

[88] Cfr. Cass. pen., sez. un., 29 gennaio 2015, n. 31022, cit., e Cass. pen., sez. II, 15 giugno 2018,

sollecitato a fronte della ricorrenza di arresti giurisprudenziali nei quali si riteneva che le garanzie costituzionali in tema di sequestro preventivo della stampa non fossero estensibili agli articoli giornalistici pubblicati sul web, perché il termine «stampa» sarebbe stato assunto dalla norma costituzionale in un'accezione ristretta, vale a dire con riferimento alla sola "carta stampata". Tale impostazione non è stata, tuttavia, condivisa da parte delle Sezioni Unite, che ritengono che in tale maniera si legittimerebbe un «irragionevole trattamento differenziato dell'informazione giornalistica veicolata su carta rispetto a quella diffusa in rete, con la conseguenza paradossale che la seconda, anche se mera riproduzione della prima, sarebbe assoggettabile, diversamente da quest'ultima, a sequestro preventivo».

In tale pronuncia, dunque, la Corte ritiene che il progresso tecnologico richieda di adottare una interpretazione evolutiva ed estensiva, eventualmente anche discostandosi da una «esegesi letterale del dettato normativo», per privilegiare un significato (nel caso, quello del termine *stampa*) che – senza risultare estraneo all'ordinamento positivo – sia nondimeno adeguato all'assetto da questo progressivamente raggiunto nel tempo; un'interpretazione *evolutiva* che, tuttavia, «non può riguardare tutti in blocco i nuovi mezzi, informatici e telematici, di manifestazione del pensiero (*forum, blog, newsletter, newsgroup, mailing list,* pagine *Facebook*), a prescindere dalle caratteristiche specifiche di ciascuno di essi, ma deve rimanere circoscritto a quei soli casi che, per i profili strutturale e finalistico che li connotano, sono riconducibili […] nel concetto di "stampa" inteso in senso più ampio»[89].

In tal senso, dunque, la Corte di Cassazione invita a non intendere il concetto di stampa «nella sua accezione tecnica di riproduzione tipografica o comunque ottenuta con mezzi meccanici o fisicochimici», ritenendo di aderire al «significato figurato» del termine, che definisce «il prodotto editoriale che presenta i requisiti ontologico (struttura) e teleologico (scopi della pubblicazione) propri di un giornale», rispetto al quale la circostanza che la pubblicazione avvenga *offline* o *online* non determina alcun mutamento significativo. Per converso, per le medesime ragioni tale interpretazione evolutiva non consente di ricondurre alla nozione di "stampa" «la diffusione di notizie ed informazioni da parte di singoli soggetti in modo spontaneo», che costituisce espressione del più generale diritto di manifestazione del pensiero[90], ma che, non assimilabile «per finalità e struttura» ad una testata giornalistica, non può essere soggetta alle

n. 39088, in *Dir. giust.,* 29 agosto 2018.

[89] Cfr. ancora Cass. pen., sez. un., 29 gennaio 2015, n. 31022, cit.

[90] Cfr. Cass. pen., sez. V, 19 febbraio 2018, n. 16751, cit.

tutele e agli obblighi previsti dalla legge sulla stampa. A tali condizioni, quindi, la Corte di Cassazione ritiene che l'interpretazione estensiva del detto termine «non esorbita dal campo di significanza del segno linguistico utilizzato ed è coerente con il dettato costituzionale»[91].

L'impostazione metodologica adottata dalla Corte si rivela estremamente significativa, dal momento che viene affrontata in termini espliciti la questione relativa alla possibilità di assimilare condotte che siano poste in essere nella "rete" e analoghe condotte che si verifichino nel mondo "fisico". L'approccio adottato nella giurisprudenza di legittimità è, in questo caso, essenzialmente funzionale, e perciò condivisibile nella misura in cui esso tende a ridimensionare la significatività in termini giuridici di differenze che si manifestino da un punto di vista esclusivamente *modale*, fintanto che esse non mutino la sostanza (*finalità* e *struttura*) del fenomeno regolato.

Tali medesime considerazioni sono state impiegate dalla Corte di Cassazione anche quando si è trattato di valutare l'eventuale responsabilità *ex* art. 57 c.p. del direttore di testate telematiche: invero, senza alcun tema di travalicare il limite dell'applicazione analogica, si è affermato che il giornale telematico, a differenza di altri mezzi informatici di manifestazione del pensiero, soggiaccia alla normativa sulla stampa, perché «*ontologicamente e funzionalmente* assimilabile alla pubblicazione cartacea», con la conseguente configurabilità della responsabilità *ex* art. 57 c.p. anche in capo al suo direttore[92]. Parallelamente, dunque, rilevando come l'unico elemento di rilievo consista nella riconducibilità della pubblicazione alla nozione di "stampa" e non, invece, nella natura dello strumento utilizzato, cartaceo ovvero virtuale, la Corte di cassazione ha escluso, in tema di diffamazione, l'applicabilità dell'aggravante dell'aver commesso il fatto con il mezzo della stampa al soggetto che abbia pubblicato un *post* diffamatorio su un *social network*, non già per la natura virtuale (anziché cartacea) dello strumento utilizzato, ma perché a carico di un soggetto che pubblichi un post su un *social network* non potranno, certo, essere imposti oneri informativi analoghi a quelli che gravano su un giornalista professionista, tenuto conto della profonda differenza fra le due figure per «ruolo, funzione, formazione, capacità espressive, spazio divulgativo e relativo contesto»[93].

In tali ultimi esempi pare, in effetti, che la Corte di Cassazione maneggi in modo molto più convincente lo strumento dell'interpretazione estensiva, per le ragioni già

[91] Cfr. Cass. pen., sez. V, 23 ottobre 2018, n. 1275, in *Guida al diritto*, 2019, 15, 85 ss.
[92] Cfr. Cass. pen., sez. V, 23 ottobre 2018, n. 1275, cit.
[93] Cfr. Cass. pen., sez. V, 19 novembre 2018, n. 3148, in *Guida al diritto*, 2019, 8, 36 ss.

indicate, e cioè per l'adozione di un approccio *funzionale*, privo della rigidità di quelle letture che valorizzano differenze meramente *materiali*, ma anche più "solido" (in ragione degli argomenti *strutturali* e *strumentali*) di quelle interpretazioni costruite su intuizioni "metaforiche". In molti casi, infatti, si è visto come l'impostazione adottata dalla Corte di Cassazione al fine di applicare le fattispecie tradizionali a nuove fenomenologie criminose si basi su *fictiones iuris*, metafore e argomenti sul filo dell'analogia, tesi a ricondurre il *cybercrime* nell'alveo della disciplina vigente e all'interno di immagini e concetti più familiari e facilmente malleabili: in tale maniera, tuttavia, non concentrandosi sulla natura sostanziale di internet ma filtrandolo attraverso immagini e figure già note, come già accaduto al legislatore, la giurisprudenza rischia di non mettere sempre a fuoco la (eventuale) specificità di ciò che accade su internet e di trascurare il fatto che le nuove tecnologie, in ragione di alcune proprie caratteristiche peculiari, abbiano reso necessario ripensare la tutela di alcuni diritti fondamentali, declinandoli secondo le peculiarità della rete[94].

6. Conclusioni: la necessaria inversione del ragionamento per la «costruzione giuridica» del *cybercrime*

All'esito dell'analisi condotta sinora, pare di potersi concludere che ciascuno dei due diversi possibili approcci alla criminalità informatica – ovverosia, la possibilità di intenderlo quale mutamento *fenomenico* rispetto alla tradizionale realtà materiale o, invece, quale mera variante *semantica* rispetto al tenore testuale della legislazione già esistente – non possieda tanto una valenza conoscitivo-descrittiva, quanto piuttosto corrisponda a una diversa visione di politica della "costruzione giuridica" del fenomeno considerato. Analogamente, come si è visto, anche il ricorso all'analogia (legislativa e giudiziale), all'interpretazione estensiva e, soprattutto, al linguaggio metaforico – ricorrenti nel settore del diritto dell'informatica – costituiscono operazioni interpretative tutt'altro che automatiche o neutrali, potendo un linguaggio all'apparenza descrittivo celare tanto un intento precettivo, quanto una determinata "precomprensione" del fenomeno da regolare.

Un simile approccio pare senz'altro aver contribuito all'attuale "frantumazione" della categoria del crimine informatico, al punto che, a causa del frequente ricorso a

[94] In relazione, ad esempio, alla peculiare declinazione del diritto alla libertà di espressione *online*, cfr. fra tutti M. BASSINI, *Internet e libertà di espressione*, Aracne Editrice, 2019.

un linguaggio inadeguato e a stilemi consolidati che hanno spesso offuscato l'essenza e le specificità del fenomeno da regolare, al nome "crimine informatico" non corrisponde alcun concetto. D'altronde, l'esigenza di pervenire a una sistematizzazione del tema, in una prospettiva sostanziale, deriva non tanto da una astratta necessità di concepire il "diritto penale del *cybercrime*" quale autonoma partizione sistematica, ma piuttosto dall'urgenza di far sì, ad esempio, che a tale fenomeno corrisponda un trattamento giuridico adeguato e omogeneo, e non, invece, come ora accade, conseguenze sanzionatorie del tutto disarticolate.

Infatti, ciascuna delle descritte concettualizzazioni, utilizzate nel discorso giuridico per classificare una nuova tecnologia, possiede e produce un significato normativo, che influisce anche in termini prescrittivi sulla modulazione della disciplina applicabile: perché il diritto (penale) dell'informatica non si riduca a un gioco di ombre cinesi è, dunque, necessario sottolineare come analogie e metafore possano semmai costituire uno strumento utile soltanto *ex post*, per semplificare la descrizione di una nuova tecnologia. Non si deve, però, pretendere di poter identificare solo sulla base dell'ombra quale sia l'oggetto che la produce.

Essenziale è, invece, che *ex ante* tanto il legislatore quanto il giudice non si limitino a guardare le sagome, che possono ingannare lo spettatore disattento, ma si confrontino direttamente con le caratteristiche sostanziali dei fenomeni che vengono in considerazione, rifuggendo dall'uso di immagini che, benché suggestive, finiscono per condizionare eccessivamente il successivo ragionamento giuridico. In altre parole, è sempre più necessario che il fenomeno tecnologico inizi a essere considerato *per ciò che è e non per ciò che sembra*, affinché la nozione di "crimine informatico" possa assumere un qualche significato.