DIRITTO PENALE CONTEMPORANEO

ISSN 2039-1676

11 maggio 2017 | Ivan Salvadori

ALISDAIR A. GILLESPIE, CYBERCRIME. KEY ISSUES AND DEBATES, OXON-NEW YORK, 2016, PP. I-VIII+308

Recensione

1. Il diritto penale dell'informatica è un territorio dello *ius puniendi* in continua evoluzione, che ricomprende un fascio sempre più ampio di fatti illeciti. Le nuove tecnologie dell'informazione e della comunicazione (di seguito: TIC), ed in specie Internet, **facilitano la commissione di reati tradizionali** (diffamazione, truffa, produzione e distribuzione di pedopornografia, ecc.) e **danno vita a nuovi fenomeni criminosi** (*sexting*, *online grooming*, *revenge porn*, ecc.). Un'opera che volesse abbracciare tutti i settori del diritto penale dell'informatica difficilmente potrebbe essere esaustiva, data l'impossibilità di affrontare, con il rigore metodologico che richiede un'indagine scientifica, i molteplici e complessi nodi dogmatici e politico-criminali che sollevano i *cyber crimes*. Ma anche qualora fosse possibile raggiungere tale obiettivo (ad es. mediante un lavoro a più mani), una tale opera sarebbe destinata a diventare rapidamente obsoleta, data la costante evoluzione della normativa penale, che i legislatori nazionali sono chiamati periodicamente ad adeguare per colmare le lacune che via via emergono dalla prassi applicativa, oltre che per dare attuazione ai sempre nuovi obblighi di incriminazione di fonte sovranazionale. Questo spiega, almeno in parte, perché in questo peculiare territorio del diritto penale tendano a prevalere contributi su tematiche settoriali o su "microsistemi normativi" (tutela della *privacy online*, danneggiamenti informatici, violazioni del *copyright*, ecc.). A prima vista, potrebbe dunque sembrare audace la scelta di Alisdair Gillespie, professore di diritto penale dell'informatica presso la *University of Lancaster-School of Law*, di dedicare una monografia al tema generale del *cybercrime*. Nella prefazione alla sua stimolante opera, l'autorevole studioso inglese ammette però che non è "*the definitive book*" sul diritto penale dell'informatica. L'obiettivo, più modesto, dell'indagine consiste, come emerge chiaramente dal sottotitolo ("*Key Issues and Debates*"), nel tentare di dare risposta alle "questioni chiave" del diritto penale che pongono le molteplici forme di manifestazione della criminalità cibernetica.

2. L'opera, che si snoda lungo undici capitoli suddivisi in quattro parti, ha ad oggetto i **fenomeni criminosi commessi in Internet o la cui realizzazione è agevolata dall'impiego delle TIC (*cyber crimes*)**. Rimangono esclusi dalla trattazione i comportamenti umani realizzati mediante o contro un *computer* non connesso alla rete (*computer crimes*) e che nell'era del *web* 2.0 sono ormai un lontano ricordo. L'A. definisce preliminarmente il concetto di *cybercrime*; affronta poi la complessa questione della **giurisdizione nel cyberspazio**; descrive quindi sotto il profilo empirico-criminologico i più rilevanti comportamenti illeciti commessi in Internet e verifica la possibilità di ricondurli nell'alveo delle fattispecie incriminatrici contemplate dall'ordinamento inglese e gallese[1]. Condivisibile è la scelta metodologica di anteporre all'analisi del dibattito dottrinale e giurisprudenziale sui reati informatici previsti in detto ordinamento, un sintetico richiamo critico ai precetti di fonte sovranazionale. Non sempre però vengono efficacemente messi in evidenza i punti in comune e le principali distonie con le prescrizioni e le raccomandazioni del Consiglio d'Europa e dell'Unione europea.

3. Nell'**assenza di un concetto dogmatico analogo a quello di bene giuridico** cui riferirsi, nei sistemi di *common law* i reati informatici, al pari di quelli "tradizionali", vengono classificati dalla dottrina sulla base di parametri criminologici, che privilegiano le modalità di commissione, le caratteristiche del soggetto agente, i motivi che lo spingono ad agire ovvero la **"funzione" che svolge il sistema informatico nella commissione del reato**. L'A., ritenendo più corretto muovere dal significato criminoso della condotta e dal risultato/effetto che essa produce, suddivide pertanto i *cyber crimes* nelle seguenti quattro categorie, a seconda che abbiano ad oggetto: 1) i sistemi informatici; 2) il patrimonio; 3) i contenuti illeciti; 4) la persona. E l'organizzazione dell'opera segue dunque questa quadripartizione.

4. Tra le molteplici minacce alla riservatezza, all'integrità e alla disponibilità dei dati e dei sistemi informatici (*CIA offences*), cui sono dedicati i tre capitoli che compongono la prima parte del volume, l'A. si sofferma sull'*hacking* ed il *cracking*, sull'intercettazione di dati informatici, sui danneggiamenti informatici, nonché sulla produzione e diffusione di *malware* (cap. 3 e 4). Tali attività delittuose vengono pacificamente ricondotte dalla dottrina e dalla giurisprudenza inglese nell'alveo della norma "a più fattispecie" di accesso non autorizzato ad un sistema informatico (sec. 1(1) *Computer Misuse Act*), che si configura come reato ostacolo (*inchoate offence*).

5. Nell'ambito dei reati contro i sistemi informatici, Gillespie analizza poi i fenomeni, di recente emersione, dell'***hacktivism***, del **cyber-terrorismo** e della **guerra cibernetica** (cap. 5). L'*hacktivim* viene equiparato, da un settore della dottrina di lingua inglese, ai tradizionali movimenti per i diritti civili ed abbraccia le forme di protesta realizzate in rete (*sit-in* virtuali, *web defacement*, utilizzo di *malware*, ecc.). Tali manifestazioni virtuali, spesso connotate politicamente, sono, di regola, penalmente rilevanti e sussumibili nelle fattispecie di accesso abusivo ad un sistema infomatico e di danneggiamento di dati e di sistemi informatici. A diversa conclusione si dovrebbe giungere, secondo l'A., rispetto agli attacchi che cagionano il blocco o l'interruzione di un servizio (*Denial of Service* e *Distributed Denial of Service attacks*) e che conseguano ad una iniziativa spontanea di migliaia di utenti i quali, previo accordo in rete, decidano di connettersi contemporaneamente ad una determinata pagina *web* (di un ente pubblico, di una multinazionale, ecc.), per ostacolare il regolare funzionamento del *Server* che la

ospita. Questi casi dovrebbero considerarsi, a suo parere, come una legittima forma di protesta o di occupazione pacifica *online*, dato che il fatto di connettersi ad un particolare sito Internet in un momento prestabilito non può essere di per sé oggetto di rimprovero penale.
Il cyber-terrorismo, quale peculiare forma di terrorismo posto in essere nel (o mediante il) *web*, persegue il principale obiettivo di colpire e ledere gli interessi degli Stati o di intimidire la popolazione civile. Sebbene non possa escludersi *a priori* la possibilità che da un attacco di matrice terroristica a sistemi informatici che gestiscono infrastrutture critiche (cd. *SCADA systems*) derivino gravi danni alla popolazione, a cose ed a beni immobili (dighe, reti elettriche, ecc.) ovvero problemi di ordine pubblico, l'A. evidenzia, a ragione, come non si possa affermare che il cyber-terrorismo rappresenti ad oggi una reale ed effettiva minaccia per la collettività. La maggior parte delle reti telematiche che gestiscono le infrastrutture critiche, non essendo accessibili via Internet, difficilmente possono essere attaccate da remoto.
Ampio spazio viene poi dedicato al complesso fenomeno, ancora inesplorato nella nostra penalistica, della guerra cibernetica. Nel dibattito di lingua inglese si discute se la *cyber warfare* sia soggetta allo *jus ad bellum* e allo *jus in bello*. Secondo Gillespie, uno Stato può invocare il diritto di autodifesa sancito dall'Art. 51 della Carta delle Nazioni Unite e ricorrere all'uso della forza cinetica per tutelare la sovranità del suo territorio soltanto qualora sia vittima di un attacco informatico i cui effetti siano paragonabili, per intensità, a quelli prodotti dalle armi tradizionali (*effects-based approach*). Qualche perplessità viene opportunamente avanzata in merito alla possibilità di applicare, nel contesto di un conflitto cibernetico, il diritto internazionale umanitario (*jus in bello*), il cui obiettivo principale è proteggere specifiche categorie di soggetti (civili, prigionieri di guerra, ecc.). Non sempre invero è possibile distinguere in modo netto tra obiettivi militari e civili, in specie laddove si tratti di tecnologie "a duplice uso" (*ISP*, reti *wi-fi*, ecc.).

6. Nella seconda parte dell'opera, dedicata ai **reati informatici contro il patrimonio**, l'A. richiama le molteplici forme di truffa commesse in Internet (cap. 6). In particolare, vengono analizzate le insidiose e molteplici forme di frode commesse nell'ambito delle aste *online*, mediante messaggi di posta elettronica ("*romance frauds*", *phishing* o "*419 fraud*") o attraverso la "clonazione" di pagine *web* (*pharming*), per verificare, nella criticabile assenza di una fattispecie *ad hoc* di frode informatica, la loro sussumibilità, tutt'altro che agevole, nel tradizionale reato di truffa (sec. 2 del *Fraud Act* del 2006).
Di seguito l'A. si sofferma sulla **normativa penale in materia di *copyright***, che coincide sostanzialmente con quella prevista nel nostro ordinamento; si pone quindi la questione se la sottrazione di beni virtuali possa essere sussunta nel delitto di furto di cui alla sec. 1 *Theft Act* del 1968 (cap. 7). Sebbene l'oggetto materiale del suddetto delitto ricomprenda anche i beni intangibili, esclude che i dati informatici, al pari delle informazioni, possano essere sottratti a chi ne abbia la disponibilità "virtuale", dal momento che la loro immaterialità ne preclude l'effettivo spossessamento. Alla stessa conclusione giunge rispetto agli oggetti immateriali (ad es. denaro o "armi" virtuali) che esistono soltanto nel cyberspazio (ad es. in *Second Life* o nell'ambito di giochi *online*).

7. La terza parte dell'opera concerne i fatti illeciti di **produzione, diffusione e commercializzazione tramite Internet di contenuti illeciti** (cap. 8). L'A. dà conto del dibattito dottrinale sul **discorso d'odio (*hate speech*)** ed in particolare sulle **pagine *web* che incoraggiano o inducono al suicidio (*suicide websites*)**, la cui creazione, in base alla sec. 2A del *Suicide Act* del 1961, modificato dal *Coroners and Justice Act* del 2009, è punita con la reclusione fino a quattordici anni. Meno diffusi in rete sono i siti dedicati all'**autolesionismo (*self-injury websites*)** e ai **disordini alimentari (*eating disorder websites*)**. La maggior parte della letteratura di lingua inglese evidenzia la pericolosità di tali pagine *web*, dal momento che le immagini ed i video in esse contenuti potrebbero avere l'effetto di incitare altri utenti (in specie adolescenti) ad emulare tali atti. L'A. non ritiene però giustificata una loro incriminazione, mancando approfonditi studi scientifici che dimostrino l'effettiva esistenza di un nesso tra la visualizzazione di tali pagine *web* e la commissione di comportamenti autolesionistici. Il "*self-harm*" non è di per sé penalmente rilevante. Di conseguenza, anche le condotte che lo pubblicizzano o lo glorificano dovrebbero considerarsi lecite.

8. Il nono capitolo è incentrato sulla produzione e diffusione in rete di **pornografia adulta** ed estrema. Di particolare interesse, data l'attualità del fenomeno, sono le pagine dedicate alla **cd. "vendetta porno" (*revenge porn*)**. L'incorporazione delle telecamere nei dispositivi (*smartphone*, *tablet*, ecc.) connessi ad Internet ha aumentato notevolmente le possibilità di produrre materiale pornografico e di caricarlo e distribuirlo sul *web*. La diffusione non consentita di tali immagini e video, al pari dei casi di voyerismo, può cagionare una grave offesa alla riservatezza, nonché all'integrità psichica e sessuale della persona rappresentata. Allo stesso tempo il *revenge porn* nega alla vittima il diritto fondamentale al controllo del suo corpo e della sua sessualità. Per contrastare tali comportamenti, sempre più diffusi anche tra i minori, il legislatore inglese, con la sec. 33 del *Criminal Justice and Courts Act* (*CJCA*) del 2015, ha previsto la reclusione fino a due anni per la rivelazione non consentita di immagini private di natura pornografica a terzi con lo scopo di causare un turbamento (*distress*) alla vittima[2].

9. Il decimo capitolo dedica particolare attenzione al controverso tema della **pornografia minorile**. L'A. esclude che la sua incriminazione possa giustificarsi sulla base del fatto che la sua fruizione incentiverebbe la commissione di ulteriori reati sessuali nei confronti dei minori, mancando approfonditi studi scientifici che dimostrino l'esistenza di tale nesso. Nega inoltre che il possesso del suddetto materiale alimenterebbe, seppur in modo indiretto, lo sfruttameno sessuale dei fanciulli. Più persuasivo ritiene l'orientamento, sostenuto da autorevole dottrina e da un filone giurisprudenziale (*R v. Beaney*, 2004), secondo cui chi dispone di immagini o video pedopornografici contribuirebbe a perpetuare il danno ("*continuing harm*") psico-fisico subito dal minore. Ed in questo senso l'A. parla di "seconda vittimizzazione": il "consumo" di pornografia minorile farebbe rivivere l'abuso sessuale di cui è stato vittima il minore. Evidenzia tuttavia come non sempre il minore sia consapevole (per la sua giovane età o per il fatto di ignorare di essere stato ripreso) dell'esistenza del materiale pedopornografico nella cui produzione è stato coinvolto.
Altrettanto controversa, per Gillespie, è la scelta politico-criminale di incriminare, con il *Coroners and Justice Act* del 2009, la pedopornografia virtuale. Un settore della dottrina ha sostenuto che la produzione e la diffusione di tale materiale contribuirebbero al consolidamento di "modelli culturali" nei quali i minori vengono ridotti a mero strumento per il soddisfacimento dei desideri sessuali degli adulti. Secondo l'A. tale tesi sarebbe poco persuasiva. L'idea che la pedopornografia virtuale porti alla progressiva reificazione e mercificazione dei minori poggerebbe, a suo dire, su argomentazioni di tipo paternalistico o moralistico. Riconosce poi che il materiale pedopornografico potrebbe essere impiegato da soggetti malintenzionati per adescare i minori. Ma tale circostanza dovrebbe servire per giustificare l'incriminazione del

child-grooming e non, come affermato da un orientamento dottrinale, del mero possesso del suddetto materiale illecito. L'unica ragione per punire la pedopornografia virtuale potrebbe dunque fondarsi, secondo l'A., su considerazioni di carattere morale: esse sarebbero però in evidente contrasto con i valori ed i principi penalistici di uno Stato laico e liberale.

10. L'undicesimo ed ultimo capitolo ha ad oggetto i principali **reati contro la persona che possono essere commessi nel *web***. Nell'assenza di norme specifiche per punire il ***cyberstalking*** e il ***cyber-bullying***, la giurisprudenza inglese tende a sussumere tali comportamenti nell'alveo delle fattispecie tradizionali che incriminano il cd. *harassment*. La sec. 127(1) del *Communications Act* del 2003 punisce, ad esempio, il fatto di inviare mediante un sistema informatico un messaggio o materiali che siano notevolmente offensivi, osceni, minacciosi o indecenti. La stessa condotta è punita se posta in essere al fine di cagionare uno stato di afflizione o di ansietà alla vittima (sec. 1(1) *Malicious Communications Act* del 1998: *MCA*) ovvero abbia ad oggetto informazioni false (sec. 1(a)(iii) *MCA*). Una fattispecie *ad hoc* in materia di *stalking* è stata introdotta nell'ordinamento inglese dal *Protection Freedom Act* del 2012, che ha modificato il *Protection from Harassment Act* del 1997 (*PfHA*). In base alla definizione legale fornita dalla sec. 7(2) *PfHA*, per *harrasment* si deve intendere ogni condotta che cagioni allarme o angoscia ad una persona. Il fatto di reato, per essere penalmente rilevante, deve essere commesso almeno due volte (sec. 2 *PfHA*). La condotta integrerà una ipotesi delittuosa più grave qualora faccia insorgere nella vittima la paura che il soggetto agente possa usare violenza nei suoi confronti (sec. 4(1) *PfHA*).
Nella seconda parte del capitolo conclusivo lo studioso britannico analizza il sempre più frequente ed insidioso fenomeno dell'**adescamento sessuale di minori in rete (*online grooming* o *sexual solicitation of a child*)**. Secondo la condivisibile definizione proposta dall'A., ed oggi prevalente nella dottrina anglosassone, il *grooming* consiste nel "processo" mediante il quale un potenziale predatore sessuale tenta di carpire la fiducia di un minore e di ottenerne il consenso alla successiva realizzazione di attività sessuali illecite. Anticipando le scelte politico-criminali del Consiglio d'Europa e dell'Unione europea, il legislatore inglese, con la sec. 15 del *Sexual Offences Act* del 2003 (di seguito *SOA*), di recente modificata dalla sec. 36 del *Criminal Justice and Courts Act* del 2015, ha punito il fatto di incontrare un minore a seguito di adescamento ("*meeting a child after grooming*"). Nello specifico la previsione legale incrimina l'adulto che comunichi, in una o più occasioni, con un minore infrasedicenne, purché a tale condotta segua un incontro ovvero il soggetto agente viaggi per incontrare il minore per scopi sessuali o quest'ultimo viaggi per trovarsi con il suo adescatore. L'A. critica la tecnica di formulazione della fattispecie, dato che il suo ambito di applicazione non si estende ai casi molto frequenti di *grooming* commessi in un contesto *online*, senza dunque che vi sia alcun contatto né attività materiale nel mondo esterno tra il predatore sessuale e la giovane vittima.

11. In conclusione, l'opera di Gillespie, fedele allo spirito anglosassone, si caratterizza per un **approccio metodologico eminentemente pratico e casistico**, con uno stile espositivo molto chiaro, che ne agevola la lettura anche a chi è poco aduso al lessico informatico e giuridico-penale. Il costante richiamo alla giurisprudenza e alle più rilevanti pronunce della Corte EDU mette in risalto le frequenti difficoltà che sorgono nella prassi per procedere all'inquadramento giuridico-penale dei sempre più complessi fenomeni criminosi connessi all'utilizzo illecito delle TIC. L'A., avvalendosi dall'apporto della dottrina più autorevole, si sforza di dare risposta a queste controverse questioni interpretative e dimostra, sulla base di alcuni casi pratici, come il diritto penale inglese, pur a fronte delle evidenti lacune (in specie in materia di intercettazioni, falsificazioni e frodi informatiche), possa applicarsi a gran parte delle nuove manifestazioni del *cybercrime*. Sicuramente maggiore sarebbe stato il contributo al dibattito in *subjecta materia* se l'A. avesse formulato delle proposte di riforma della legislazione penale inglese, anche alla luce della ricca esperienza giuridica dei sistemi di *common law* più all'avanguardia nella lotta alla criminalità informatica (quali gli Stati Uniti, il Canada e l'Australia). Opportuna sarebbe poi stata la previsione di un capitolo conclusivo, nel quale formulare un giudizio finale sull'attuazione, nell'ordinamento interno, dei precetti di fonte europea e sulle discutibili tecniche di incriminazione, nonché scelte politico-criminali del legislatore inglese in questo ambito: in specie su quelle che prevedono una notevole anticipazione della soglia di rilevanza penale mediante l'ampio ricorso alla tecnica dei reati ostativi o preparatori (*inchoate offences*, *possession offences*, *preparatory offences*, *proxy crimes*, *prophylactic crimes*, ecc.). In tal senso avrebbe sicuramente giovato un'indagine critica del contenuto offensivo di tali fattispecie, correlabile al ricco e vivace dibattito dottrinale anglosassone sul cd. *remote harm* e sulle diverse tipologie incriminatrici riconducibili al cd. diritto penale preventivo (*preventive criminal law*)[3]. L'opera di Gillespie rappresenta comunque, anche per lo studioso italiano, una stimolante lettura per cogliere le complesse sfide che il *cybercrime* pone non solo al legislatore, che deve garantire risposte adeguate alle nuove minacce che derivano dall'utilizzo illecito delle nuove tecnologie per i beni tradizionali e di nuova emersione nella società dell'informazione, ma anche alla giurisprudenza e alla dottrina, tenute a vigilare sulla conformità delle scelte politico-criminali adottate in questo peculiare territorio dello *ius puniendi* ai principi penalistici di rango costituzionale e convenzionale/sovranazionale, nonché sul rispetto dei diritti e delle libertà fondamentali degli utenti della rete.

[1] Si ricordi che il diritto penale inglese si applica anche al Galles. La Scozia conserva invece un'autonomia legislativa in ambito penale.
[2] Il legislatore ha previsto che il fatto non costituisca reato qualora il soggetto agente, pur essendosi rappresentato la concreta possibilità che la divulgazione del materiale potesse arrecare un danno alla vittima, non abbia agito per perseguire quello scopo. Ha previsto altresì alcune cause di non punibilità (*defences*) qualora il soggetto agente abbia ragionevolmente creduto che la rivelazione delle immagini fosse necessaria per prevenire, scoprire o investigare un reato (sec. 33(3) *CJCA*); vi fosse un interesse pubblico nel divulgarle nell'ambito di un'indagine giornalistica (sec. 33(4) *CJCA*) ovvero non vi fosse ragione per credere che mancasse il consenso dell'interessato alla divulgazione delle immagini.
[3] In tal senso v., nella ormai copiosa letteratura, gli autorevoli contributi di Simester A.P., Von Hirsch A., *Remote Harms and Non-constitutive Crimes*, in *Crim. Just. Ethics*, vol. 28, Issue 1, 2009, p. 89 ss.; ID., *Crimes, Harms, and Wrongs. On the Principles of Criminalization,* Oxford, 2011; Ashworth A., L. Zedner, *Just Prevention: Preventive Rationales and the Limits of the Criminal Law*, in R.A. Duff, S.P. Green (eds.), *Philosophical Foundations of Criminal Law*, New York 2011, p. 279 ss.; ID., *Prevention and Criminalization*: *Justifications and Limits*, in *New Crim. L. Rev*., vol. 15, Issue 4, 2012, p. 542 ss.; Duff R.A, Marshall S.E., *'Remote Harm' and the Two Harm Principles*, in A.P. Simester, U. Neumann, A. Du Bois-Pedain (eds.), *Liberal Criminal Theory. Essays for Andreas von Hirsch*, Oxford 2014, p. 205 ss.