Cybersecurity, (auto)regolazione e governance del rischio. Quid de iure poenali?

di **LUCA D'AGOSTINO**

SOMMARIO: **1.** DALLA *CYBERLAW* ALLA *CYBERSECURITY* – **1.1.** UNA DEFINIZIONE NORMATIVA – **2.** *CYBER-RISK* E DIRITTO PENALE – **3.** IL RUOLO DELL'AUTODISCIPLINA E DELLA *COMPLIANCE* NEL SETTORE DELLA PROTEZIONE CIBERNETICA E DELLA SICUREZZA DELLE INFORMAZIONI: RIFLESSI IN TERMINI DI RESPONSABILITÀ PENALE – **4.** LA DIRETTIVA C.D. *NIS* E LE PROSPETTIVE DI TUTELA PENALE – **5.** CONCLUSIONI.

Abstract

The enactment of directive 2016/1148/UE concerning *"measures for a high common level of security of network and information systems across the Union"* raised the necessity of the implementation of cybersecurity national strategies, imposing risk prevention duties for operators of essential services and digital service providers, and, in case of violation, effective, proportionate and dissuasive penalties against the obliged professionals.
Starting from the arrangement of a legal definition of cybersecurity, after analysing the impact of self-regulation on individual criminal liability, the Author evaluates the new Directive impact on corporate cyber-risk compliance duties, and the emergent liabilities for failure to adopt organizational and technical measures.

1. Dalla cyberlaw alla cybersecurity. I nuovi mezzi di comunicazione e di informazione manifestano in modo sempre più intenso la dimensione "pervasiva" e "globalizzante" (PICOTTI, 2012) del cyberspazio. *Internet* è da sempre considerato un fattore di garanzia e libertà per gli utenti del mondo digitale. Ma nella moderna società dell'informazione esso rappresenta anche un indubbio fattore di rischio per i diritti fondamentali degli individui.

La dicotomia in parola è stata metaforicamente svelata da un compianto Maestro, la cui parole tornano sonore alla mente. *«La rete […] porta con sé anche un'impostazione, più che ideologica, mitologica, che sembra evocare la lancia di Achille e quella di Parsifal, armi capaci di offendere e guarire";* una mitologia che però viene smentita *"da una realtà nella quale non solo Internet è variamente oggetto di regolazione, ma soprattutto conosce violazioni continue di quello statuto di libertà che si riteneva poter essere affidato alla propria, esclusiva virtù salvifica»* (RODOTÀ, 2010).

La regolazione della rete viene attuata mediante la *cyberlaw* (ZICCARDI, 2011) che, in senso lato, viene intesa come il complesso di disposizioni che disciplinano il rapporto tra utenti del mondo digitale al fine di proteggere interessi di primaria importanza come la personalità individuale, la riservatezza delle comunicazioni, la confidenzialità delle informazioni, i dati personali, il diritto d'autore.

Negli ultimi anni la *ITC policy* internazionale si è evoluta in senso "funzionalistico", abbandonando l'idea di un intervento statico e strettamente regolatorio – e quindi la *cyberlaw* nel senso sopra richiamato – in favore di un approccio più "eclettico" e dinamico di tutela. La diffusione del concetto di *cybersecurity* riflette al contempo un fenomeno culturale e un'esigenza della moderna società dell'informazione; lungi dal poter essere ridotta a mero valore di principio, la *cybersecurity* è la risposta "sociale" alla crescente informatizzazione dei processi comunicativi e dei rapporti economici e, con essi, all'aumento del rischio di *cybercrime*. Le statistiche più recenti evidenziano come la criminalità informatica abbia assunto dimensioni draconiane, destinate ad una ulteriore superfetazione in difetto di adeguate misure di prevenzione (SEVERINO, 2017)[1].

1.1 Una definizione normativa. La nota distintiva di questa nuova materia è indubbiamente la trasversalità[2] che la caratterizza.

L'attuazione di un elevato *standard* di sicurezza informatica, specie ove riferito a organizzazioni complesse, richiede una sinergia di competenze di carattere tecnico, economico, giuridico. Si può quindi affermare che la

1 Le statistiche diffuse dal *World Economic Forum* hanno stimato il costo globale della criminalità informatica in 445 miliardi di dollari all'anno, e che, in mancanza di efficaci strategie difensive e preventive nel 2020 le perdite economiche causate dalla criminalità informatica potrebbero arrivare fino a 3.000 miliardi di dollari. Cfr. Consorzio Interuniversitario per l'informatica (CINI) nel documento *Il futuro della Cybersecurity in Italia*, ottobre 2015, p. 2.

2 In questo senso il *Rapporto CLUSIT* (Associazione Italiana per la sicurezza informatica) per l'anno 2016, p. 12 che definisce la *cybersecurity* come *"il gruppo di attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali non informatiche, che sono oggettivamente di difficile integrazione con le prassi esistenti […] costruite negli anni a partire da esigenze di compliance".* Il documento è disponibile in *open access* sul portale dell'Associazione al seguente collegamento:
https://clusit.it/wp-content/uploads/download/Rapporto_Clusit%202016.pdf

cybersecurity, condividendo il metodo di ciascuna delle scienze che la riguardano (CARCATERRA, 2011), sia una scienza derivata[3]; in quanto tale essa avrà una definizione propria e obiettivi specifici per ciascun settore di riferimento.

Ciò che interessa, ai nostri fini, è tracciare una definizione valida sul piano giuridico, che possa essere assunta a premessa maggiore del ragionamento sui possibili risvolti penalistici della *cyber-governance*. Il terreno è reso scivoloso dall'assenza di una caratterizzazione, a livello legislativo, della materia. Soltanto negli ultimi anni il legislatore ha cominciato a muovere i primi passi nel settore della "protezione cibernetica" e della "sicurezza informatica"[4] mediante interventi a carattere generale e di natura programmatica. Venendo ai tempi più recenti, l'emanazione della Direttiva 2016/1148/UE (di seguito, Direttiva NIS), rende imminente una organica rivisitazione legislativa e l'adozione di un Piano Nazionale di sicurezza informatica; l'intervento riformatore offrirà l'occasione per una più compiuta definizione normativa della *cybersecurity*. Allo stato attuale essa può essere definita come quella scienza *«che consente a una entità (ad esempio, organizzazione, cittadino, nazione ecc.) la protezione dei propri asset fisici e la confindezialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal cyber space»*[5]*.*

3 Si assume a base la nozione sociologica di scienza come astrazione di un insieme di cognizioni in un insieme di concetti elaborati attraverso un metodo. Se, sulla scorta di tale definizione, si considerano "scienze" l'informatica, l'economia e il diritto, non vi è dubbio che la *cybersecurity* condividerà anch'essa la medesima natura: essa è quindi una scienza derivata, caratterizzata da un metodo 'eclettico' e condiviso; un metodo che si fonda tanto sulle leggi positive, quanto su quelle della logica e della tecnica.

4 Il riferimento è al Piano Nazionale per la protezione cibernetica e la sicurezza informatica, approvato dal Governo nel dicembre 2013 e disponibile sul sito *internet* istituzionale dell'AgID *http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/piano-nazionale-cyber_0.pdf*

5 Così il *Framework Nazionale di Cybersecurity*, adottato dal CIS (*Cyber intelligence and information security*) dell'Università La Sapienza di Roma e dal CINI (Consorzio interuniversitario nazionale per l'informatica), con la collaborazione dell'Agenzia per l'Italia Digitale, dell'Autorità Garante per la protezione dei dati personali e il Ministero dello Sviluppo Economico; il documento è disponibile sul sito internet del Governo https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/un-framework-nazionale-per-la-cyber-security.html.

Per la precisione, il *Framework Nazionale* definisce la *cybersecurity* come "pratica", al quale abbiamo sostituito, per le ragioni anzidette, l'appellativo "scienza".

2. Cyber risk e diritto penale. La definizione contenuta nel Framework nazionale appare estremamente pertinente per una riflessione sui possibili riflessi della *cybersecurity* sul piano del diritto penale.

Anzitutto, essa focalizza l'attenzione sulle oggettività giuridiche rilevanti, quali la tutela degli *asset* fisici, delle confidenzialità e dell'integrità/disponibilità delle informazioni. Ciò, dal punto di vista del penalista, è indicativo della diversificazione dei beni protetti e, quindi, dei titoli di reato da considerare.

In secondo luogo, la definizione fa espresso riferimento alle minacce che derivano dal cyberspazio, mettendo in luce il rapporto "genetico" di causa-effetto esistente tra *cybercrime* e *cybersecurity*.

Detto rapporto, tuttavia, non si esaurisce nella sola derivazione di quest'ultimo dalla prima, anzi può essere considerato *in fieri*, nel senso che la regolazione pubblica del settore della sicurezza informatica incide sull'estensione di alcune fattispecie di reato e, sotto certi aspetti, apre nuovi orizzonti di criminalizzazione. Viene quindi in rilievo il concetto di *cyber-risk* sul quale l'interprete è chiamato a riflettere per analizzare i possibili riflessi della regolazione sul piano della responsabilità. Sotto questo aspetto, si deve rimarcare la crescente importanza che l'autoregolazione societaria assume nel contesto della *governance* del suddetto rischio

Non si deve infatti dimenticare che, da un punto di vista economico-istituzionale, la *cybersecurity* origina da esigenze di *compliance* a partire da strumenti propri della sicurezza informatica "tradizionale"[6]; per questo motivo anche il profilo l'autodisciplina riveste un ruolo fondamentale nell'implementazione di un *standard* elevato di sicurezza.

Sul piano teorico, quindi, il panorama normativo attuale non consente di delineare una autonoma nozione di *diritto penale della sicurezza informatica* al pari di altre branche (diritto penale dell'economia, del lavoro, delle biotecnologie, dell'ambiente). Ciascuna di queste è caratterizzata dalla presenza di fattispecie penali "di chiusura" di un sottosistema normativo (o più

6 Cfr. *Rapporto CLUSIT* per l'anno 2016, *cit.* p. 12

sottosistemi normativi integrati) e delle regole proprie del settore[7]. La sicurezza informatica – almeno *de lege lata* – non gode di un tessuto normativo organico e, tantomeno, di disposizioni incriminatrici che strettamente la riguardano. Ma pur negando l'esistenza di un autonomo sottosistema, la *cybersecurity* conserva comunque una incidenza indiretta sul piano del diritto penale. L'imposizione di determinati obblighi di protezione e la fissazione di un determinato *standard* di sicurezza diviene rilevante per l'integrazione di alcuni elementi qualificanti (es. il concetto normativo di colpa o di obbligo impeditivo) ovvero per la configurabilità di fattispecie penali appartenenti a settori "contigui" (es. gli illeciti in materia di trattamento dei dati personali; i delitti in materia di rivelazione dei segreti).

Inoltre – esaminando la questione *de lege ferenda* – sembra che la *cybersecurity* sia prossima ad essere riconosciuta da una fonte di rango primario per effetto del recepimento della Direttiva *NIS*; ciò potrebbe aprire nuovi ed importanti scenari d'interesse per il penalista.

3. Il ruolo dell'autodisciplina e della compliane nel settore della protezione cibernetica e della sicurezza delle informazioni: riflessi in termini di responsabilità penale. La *compliance* della sicurezza informatica assume notevole importanza sul piano della responsabilità individuale[8].

Dal punto di vista semantico essa viene definita come *«aderenza alle norme e alle prescrizioni di autoregolamentazione»*[9]*.* La *compliance* si fonda

7 Così, ad esempio, gli illeciti contravvenzionali previsti dal D. Lgs. n. 81/2008 costituiscono il corredo sanzionatorio per la violazione delle disposizioni del sistema prevenzionistico degli infortuni sul lavoro; gli artt. 216 e seguenti della legge fallimentare puniscono la sottrazione, da parte dell'imprenditore, delle garanzie patrimoniali che le procedure concorsuali mirano a garantire; gli illeciti in materia di scarico o emissione nell'aria o nelle acque puniscono la violazione delle rispettive regole di condotta fissate dal D. Lgs. n. 152/2006; i reati previsti dagli artt. 12 e 13 della legge n. 40/2004 e dall'art. 22 della legge n.91/1999 comminano una pena a chi violi le disposizioni relative alla fecondazione medicalmente assistita o quelle sui trapianti etc.

8 L'importanza delle fonti di autoregolazione è oggi ribadita dal "considerando" n. 44 della Direttiva c.d. NIS (si veda infra), secondo cui *«è opportuno promuovere e sviluppare attraverso adeguati obblighi regolamentari e pratiche industriali volontarie una cultura della gestione del rischio, che comprende la valutazione del rischio e l'attuazione di misure di sicurezza commisurate al rischio corso».*

9 Dizionario di Italiano, Garzanti, voce *Compliance*, 2010, p. 728

quindi su disposizioni di scaturigine endosocietaria – o più in generale, privata – le quali, indirettamente, incidono sulla portata di norme vincolanti di emanazione pubblica (DE BENEDETTO, 2005)[10]. L'autoregolazione colma gli spazi lasciatigli dalla regolazione e supplisce, talvolta, alle carenze di essa (BOSI, 2009): nessun processo di azione sociale potrebbe essere completamente autonomo, né interamente eteronomo (MAGGI, 2003). Ciò risulta tanto più vero nelle organizzazioni complesse nelle quali, da una parte, l'azione giuridica risulta vincolata dal sistema di regole istituzionali che la governano; dall'altra il ruolo di chi decide e l'apparato gerarchico di riferimento possono dar luogo ad un sistema di autoregolazione (ZANIER, 2012).

L'incidenza delle regole di condotta "autodisciplinari" sulla latitudine della responsabilità penale sembrerebbe scontrarsi con un limite insuperabile: il rispetto del principio di legalità, in base al quale gli elementi costitutivi della fattispecie di reato debbono essere dettati da una norma primaria di legge (PALAZZO,1999; MANTOVANI, 2002). Invero, tale principio non esclude che le fonti di autoregolazione siano prese in considerazione per il tramite di elementi normativi "elastici" della fattispecie (MARANI, 2014; RISICATO, 2004)[11], o di clausole generali (CASTRONUOVO, 2012), e che esse conformino, in tal modo, la portata della disposizione incriminatrice.

Venendo ora al tema che ci occupa, si possono richiamare alcune ipotesi in cui l'autoregolazione nel settore della sicurezza informatica incide sulla responsabilità penale dei destinatari delle regole di condotta.

Considerando la *cybersecurity* dalla prospettiva della protezione delle confidenzialità e della disponibilità di informazioni possono addursi due esempi:

10 Quella che, comunemente, viene definita "regolazione". La nozione di regolazione cui facciamo riferimento è quella delineata dall'OCSE come «*the diverse set of instruments by wich governments set requirements in enterprises and citizens».* Cfr. OCSE*, Report on Regulatory Reform*, Parigi, 1997, p. 6.
Il documento è disponibile sul sito internet istituzionale al seguente collegamento: *https://www.oecd.org/gov/regulatory-policy/2391768.pdf*

11 Il primo autore definisce "elastici" gli elementi che esprimono concetti che ammettono un margine di possibili soluzioni opposte, dipendenti dall'apprezzamento del giudice, margine che, però, non priva la norma della sua sufficiente determinatezza. La seconda, invece, definisce tali quelli la cui interpretazione è contraddistinta da una duplice linea di confine, una zona grigia all'interno della quale confluisce una gamma di accezioni affidate, per la loro concreta definizione, alla sensibilità del singolo interprete.

l'accesso abusivo a sistema informatico (art. 615-*ter* c.p.) per quel che riguarda la *compliance* nel settore privato; l'agevolazione colposa nella rivelazione di segreti d'ufficio (art. 326, comma 2, c.p.) con riferimento al contesto pubblico.

Quanto alla prima, la fattispecie punisce *«chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo».*

Si pensi ora al caso in cui una società adotti, a tutela del *know-how*, un regolamento interno sull'utilizzo di una piattaforma informatica contenente informazioni di carattere commerciale sui propri prodotti. Detto regolamento prevede che i dipendenti possano accedervi soltanto per finalità strettamente connesse al servizio, qualora autorizzati da un dirigente. La violazione delle predette disposizioni potrebbe comportare, di là dell'apertura del procedimento disciplinare, una qualche conseguenza sul piano penale?

La giurisprudenza maggioritaria ritiene il reato integrato anche dalla condotta del soggetto che, pur munito di regolare *password* – e dunque legittimato ad accedere al sistema – si introduca o si mantenga in esso per ragioni o finalità diverse da quelle giustificatrici dell'accesso e ciò in violazione delle specifiche disposizioni dettate dal titolare del sistema (FERRETTI, 2015)[12]. La norma, in realtà, aveva dato luogo ad un contrasto interpretativo, risolto dalle Sezioni Unite (PECORELLA, 2012; per gli orientamenti precedenti CUOMO, IZZI, 2002)[13] nel senso che l'accesso e il trattenimento nel sistema informatico è

12 Cfr. Cass. Pen., Sez. V, 11 marzo 2015 n. 32666, la quale ha affermato che *«nel caso di soggetto munito di regolare password, è necessario accertare il superamento, su un piano oggettivo, dei limiti e, pertanto, la violazione delle prescrizioni relative all'accesso ed al trattenimento nel sistema informatico, contenute in disposizioni organizzative impartite dal titolare dello stesso, indipendentemente dalle finalità soggettivamente perseguite».*

13 Cass. Pen., Sez. Un., 27 ottobre 2011 n. 4694 in *Cass. Pen*. 2012, 11, p. 3681ss. Il Consesso era stato chiamato a pronunciarsi *«se integri la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto abilitato ma per scopi o finalità estranei a quelli peri quali la facoltà di accesso gli è stata attribuita».* In seno alla Suprema Corte vi era infatti un orientamento che escludeva, in ogni caso, che il reato di cui all'art. 615-*ter* c.p. fosse integrato dalla condotta del soggetto il quale, avendo titolo per accedere al sistema, se ne avvalga per finalità estranee a quelle di ufficio (cfr. *ex multis* Cass. Pen. Sez. V, 20 dicembre 2007 n. 2534, in *Riv. Pen.,* 2008, 6, p. 655 ss). Un secondo orientamento riteneva invece rilevante, ai fini dell'integrazione del reato *de quo*, anche la condotta del soggetto che, pure

abusivo allorquando l'agente violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema. La nozione di "prescrizioni" viene specificata dalla Corte facendo riferimento alla violazione delle prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro[14].

Ecco dunque che le fonti di autoregolazione circa l'utilizzo del sistema informatico – e quelle che, più in generale disciplinano l'accesso ad informazioni riservate – incidono sulla portata estensiva del precetto penale. Così, nel caso pocanzi esemplificato, la violazione delle procedure interne dettate dal regolamento concorrerà a qualificare l'accesso come "abusivo" in senso penalistico.

Il secondo esempio riguarda la sicurezza sotto il profilo della tutela della confidenzialità delle informazioni apprese dai pubblici agenti. L'adozione di modelli di *cybersecurity* incide sull'accertamento della colpa nella condotta di agevolazione prevista dal secondo comma dell'art. 326 c.p.

Si pensi al caso in cui il dirigente di un ente pubblico, dopo aver salvato sul *pc* alcuni documenti segreti che riguardano il proprio ufficio, disattivi (o ometta di attivare) il *firewall*, non esegua gli aggiornamenti dell'*antivirus,* oppure ometta di proteggere l'accesso con chiavi segrete. *Quid iuris* se il computer è colpito da un attacco informatico o diviene oggetto di un accesso abusivo con il quale terzi si impossessano dell'informazione segreta?

Il codice penale punisce il pubblico agente che *«violando i doveri inerenti alle funzioni o al servizio, o comunque abusando della sua qualità, rivela notizie*

essendo abilitato ad accedere al sistema informatico o telematico, vi si introduca con la *password* di servizio per raccogliere dati protetti per finalità estranee alle ragioni di istituto ed agli scopi sottostanti alla protezione dell'archivio informatico, utilizzando sostanzialmente il sistema per finalità diverse da quelle consentite (cfr. *ex plurimis* Cass. Pen. 07 novembre 2000 n. 12732 in *Cass. Pen*. 2002, p. 1015).

14 Il tema è ancora "caldissimo" in giurisprudenza. Lo scorso 18 maggio 2017 le Sezioni Unite sono state chiamate a pronunciarsi "se integri il delitto previsto dall'art. 615-*ter*, secondo comma, n. 1, cod. pen. la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l'accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita". Al quesito è stata data risposta affermativa, su parere conforme del Procuratore Generale, con sentenza n. 41210 depositata lo scorso 08 settembre 2017.

di ufficio, le quali debbano rimanere segrete, o ne agevola in qualsiasi modo la conoscenza» (art. 326, comma 1), ciò anche *«se l'agevolazione è soltanto colposa»* (art. 326, comma 2). È opinione diffusa che la condotta di agevolazione sia integrata anche dal semplice lasciare incustodito (ANTOLISEI, 2008; ROMANO, 2013; FIANDACA, MUSCO, 2012) il documento contenente l'informazione segreta; nel caso di documento in formato digitale l'omessa custodia avrà riguardo alla mancata adozione di misure di protezione di carattere informatico.

La *governance* del cyber rischio nel contesto pubblico è disciplinata da disposizioni di particolare rilevanza (SEVERINO, 2017). Sulla Gazzetta Ufficiale sono state di recente[15] pubblicate le *"Misure minime di sicurezza ICT per le Pubbliche Amministrazioni"*[16] le quali costituiscono parte integrante delle Linee Guida per la sicurezza ICT. Il documento riporta una serie di tabelle[17] sulle disposizioni tecniche e i protocolli informatici di base, lasciando alla discrezionalità di ciascuna Amministrazione l'attività di valutazione del rischio e la concreta attuazione di misure ulteriori di tutela[18].

Tale fonte di (auto-)regolazione pubblica del *cyber risk* istituisce una sorta di "paradigma cautelare" di base, rimettendo alle singole amministrazioni la concreta attuazione di misure più incisive. Il riconoscimento di uno *standard* a livello internazionale accredita l'idea che le misure minime di sicurezza trovino

15 *Gazzetta Ufficiale della Repubblica Italiana,* Serie Generale, 04 aprile 2017, n. 79 p. 50 ss.

16 Il documento, varato in attuazione della Direttiva del Presidente del Consiglio dei Ministri del 1 agosto 2015, costituisce *«un'anticipazione urgente della regolamentazione completa in corso di emanazione, al fine di fornire alle pubbliche amministrazioni dei criteri di riferimento per stabilire se il livello di protezione offerto da un'infrastruttura risponda alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento»*. La Direttiva del 2015 aveva sollecitato tutte le Amministrazioni a dotarsi, secondo una tempistica definita e comunque nel più breve tempo possibile, di *standard* minimi di prevenzione e reazione ad eventi cibernetici. A fine di agevolare tale processo l'Agenzia per l'Italia Digitale
è stata impegnata a rendere prontamente disponibili indicatori degli *standard* di riferimento.

17 Si prevedono diverse "classi" di misure, in base agli indicatori forniti dall'Agenzia per l'Italia Digitale (c.d. *AgID Basic Security Controls*, ABSC). Questi ultimi, a loro volta, si riportano all'insieme di controlli (noto come SANS 20), pubblicati dal *Center for Internet Security*, con la denominazione *Critical Security Controls for Effective Cyber Defense* nella versione 6.0 di ottobre 2015

18 Il documento prevede, infatti, che ciascuna amministrazione *"dovrà avere cura di individuare al suo interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, all'interno dei quali potrà applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi"* (p. 54).

ragione in una valutazione di prevedibilità ed evitabilità dell'evento – sia essa la perdita o la diffusone dei dati – secondo la comune esperienza degli esperti del settore.

Nel caso esemplificato, il dirigente che abbia agevolato la presa di conoscenza altrui del documento informatico omettendo di adottare le doverose cautele sarà rimproverabile per colpa specifica, consistita nel non essersi adeguato alle disposizioni appartenenti alla prima classe delle misure minime[19]. Il modello di regolazione pubblica della sicurezza ICT è quindi rilevante per accertamento della responsabilità del pubblico agente, potendo rientrare tra le "discipline" richiamate dall'art. 43 c.p. (FORTI, 1990; BONAFEDE, 2005; CASTRONUOVO, 2009).

I casi che abbiamo esaminato mettono in evidenza che la *compliance* in materia di *cybersecurity,* è in grado di incidere sulla configurabilità, in termini oggettivi e soggettivi, dell'illecito penale, e che ciò è vero tanto nel settore privato quanto in relazione all'autoregolazione nell'ambito delle P.A.

In conclusione, l'assenza di fattispecie incriminatrici *ad hoc* e di una organica disciplina di settore non sembra essere d'ostacolo alla rilevanza "esterna" della *cybersecurity* nel riempire di contenuto gli elementi normativi di alcune fattispecie penali.

4. La Direttiva c.d. NIS e le prospettive di tutela penale. Soltanto in tempi recenti la *cybersecurity* – abbandonato l'alveo della *compliance* societaria – si è affermata a livello legislativo.

Più precisamente, guardando all'ordinamento eurounitario, l'adozione della direttiva 2016/1148/UE *(misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione)* ha segnato un passo decisivo verso l'armonizzazione delle legislazioni degli Stati membri nel settore della sicurezza delle reti e dei sistemi di informazione.

19 Che prevedono, tra gli altri, l'obbligo di dotare il sistema informatico di chiavi di accesso e di protezione dall'attacco di virus in base alle disposizioni del SANS 20.

Nel disciplinare gli obblighi cui saranno tenuti gli Stati membri, il legislatore europeo valorizza la centralità della *governance*[20] del rischio cibernetico. Infatti, per conseguire e mantenere un livello elevato di sicurezza della rete e dei sistemi informativi è anzitutto opportuno che *«ogni Stato membro disponga di una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi che definisca gli obiettivi strategici e gli interventi strategici concreti da attuare»*[21]*,* e che la pianificazione degli obiettivi sia resa effettiva mediante l'istituzione di un'Autorità nazionale competente responsabile di soddisfare i compiti connessi alla sicurezza delle reti e dei sistemi informativi (artt. 7 e 8)[22]. Essendo la sicurezza delle reti e delle informazioni un'esigenza comune al settore pubblico e a quello privato, vengono incoraggiante forme di cooperazione spontanea, anche grazie al coordinamento dell'ENISA e delle Autorità nazionali (artt. 10 e 11).

La responsabilità di garantire la sicurezza delle reti e dei sistemi informativi incombe in larga misura sugli operatori di servizi essenziali e sui fornitori di servizi digitali che sono i principali destinatari degli obblighi di prevenzione e notifica degli incidenti. Con riferimento all'attività svolta da queste categorie di soggetti, il legislatore dell'Unione riconosce l'importanza della prevenzione del *cyber-risk* (SEVERINO, 2017)*,* attribuendo rilievo all'adozione di regolamenti interni e prassi industriali: una cultura della gestione del rischio, che comprende la valutazione del rischio e l'attuazione di misure di sicurezza commisurate al rischio (SEVERINO, 2017)[23]. L'art. 14 dispone infatti che gli Stati debbano provvedere affinché gli operatori di servizi essenziali adottino «*misure tecniche e organizzative adeguate e proporzionate alla*

20 L'art. 7, par. 1, lett. b) prevede che il piano strategico nazionale debba predisporre *«un quadro di governance per conseguire gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti»*.

21 Così il "considerando" n. 29

22 Il legislatore europeo vuole che ciascuno Stato si doti delle capacità tecniche e organizzative necessarie a prevenire, individuare, rispondere e attenuare i rischi e gli incidenti a carico delle reti e dei sistemi informativi. Pertanto gli Stati dovranno anche assicurare la disponibilità di squadre di pronto intervento informatico («CERT»), in modo da garantire l'esistenza di capacità effettive e compatibili per far fronte ai rischi e agli incidenti e garantire un'efficiente collaborazione a livello di Unione (Cfr. "considerando" n. 35).

23 In tal senso si veda il "considerando" n. 44

gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni» (par. 1) e *«misure adeguate per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurare la continuità di tali servizi»* (par. 2). Non diversamente, il successivo art. 16, par. 1, prevede che i fornitori di servizi digitali *«identifichino e adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano».*[24]

Quanto alle implicazioni in termini di responsabilità individuale e collettiva del *framework* delineato dalla Direttiva *NIS*, è bene evidenziare che all'orizzonte si intravedono scenari di indubbio interesse per il penalista. Ciascuno Stato membro sarà tenuto a comminare sanzioni effettive, proporzionate e dissuasive in caso di violazione delle disposizioni nazionali di attuazione[25].

Pur non intervenendo direttamente in materia penale ai sensi dell'art. 83 TFUE[26] – e dunque lasciando alla discrezionalità degli Stati membri l'individuazione della natura dell'illecito – la Direttiva apre le porte alla eventuale introduzione di fattispecie sanzionatorie di penalistico rilievo, indipendentemente dal *nomen iuris* che il legislatore intenderà attribuir loro. Se si guarda alla coerenza sistematica con la disciplina in materia di protezione dei dati personali – specie per quel che riguarda l'adozione di misure minime di sicurezza, l'osservanza dello *standard* previsto dal Regolamento[27], e la

24 La disposizione precisa che, tenuto conto delle conoscenze più aggiornate in materia, le misure "prevenzionistiche" debbano assicurare un livello di sicurezza della rete e dei sistemi informativi adeguato al rischio esistente, tenendo conto dei seguenti elementi: a) la sicurezza dei sistemi e degli impianti; b) trattamento degli incidenti; c) gestione della continuità operativa; d) monitoraggio, audit e test; e) conformità con le norme internazionali.

25 L'art. 21 della Direttiva dispone che *«gli Stati membri stabiliscono le norme relative alle sanzioni da irrogare in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva e adottano tutti i provvedimenti necessari per la loro applicazione. Le sanzioni previste sono effettive, proporzionate e dissuasive».*

26 La *cybersecurity* è materia fortemente connessa alla prevenzione della criminalità informatica. La violazione delle disposizioni sulla sicurezza delle reti e delle informazioni, in linea di principio, ben potrebbe rientrare nelle sfere di criminalità per le quali l'art. 83, par. 1, del Trattato sul Funzionamento dell'Unione Europea ammette la fissazione di *minimum rules*. Una competenza in materia penale nel settore *de quo* potrebbe comunque ricondursi alla *annex compentence* di cui al par. 2 del medesimo articolo.

27 L'omissione di misure di sicurezza, l'inottemperanza ai provvedimenti dell'Autorità Garante e violazione dei diritti degli interessati soggiacciono alle sanzioni previste dall'art. 83, par. 5:

violazione degli obblighi di notifica dei *data breach*[28] – è dato credere che agli operatori dei servizi essenziali e ai fornitori di servizi digitali saranno imposte sanzioni estremamente onerose in caso di mancata attuazione delle misure tecniche. Dalla prospettiva della tutela dei dati personali *digital privacy* e *cybersecurity* costituiscono un sistema integrato di protezione, caratterizzato da reciproche interferenze e punti di contatto[29]: ne consegue che le fattispecie di illecito di futura introduzione *ex* art. 21 cit., dovrebbero prevedere sanzioni particolarmente incisive a carico dei soggetti destinatari degli obblighi di protezione e prevenzione.

Il tema della gravosità delle sanzioni richiama alla mente il concetto di *matière pénal* plasmato dalla giurisprudenza della Corte di Strasburgo a partire dalla storica sentenza *Engel* fino agli approdi più recenti (VIGANÒ, 2017; SCAROINA 2015; FLICK, NAPOLEONI, 2015; TRIPODI, 2014)[30]. Verrebbe quindi a

sanzione amministrativa fino a 20 000 000 EUR e, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente.
Il Trattamento non conforme alle disposizioni del Regolamento e violazione dei diritti degli interessati sono punite dall'art. 83, par. 4, con sanzioni amministrative fino a 10 000 000 EUR, e, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente.

28 È definito *data breach* «*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati». (*art. 7 Regolamento 2016/679/UE*);* la violazione dei dati personali fa sorgere l'obbligo di notifica all'Autorità di controllo (art. 33), la cui inottemperanza è sanzionata dall'art. 83, par. 4 del Regolamento Generale.

29 Non a caso l'art. 8, par. 6, della Direttiva *NIS* dispone che *«ove opportuno e conformemente al diritto nazionale, le autorità competenti e il punto di contatto unico consultano le autorità di contrasto e le autorità per la protezione dei dati nazionali competenti e collaborano con esse».*

30 La questione, ancora oggi al centro di un copioso dibattito scientifico, concerne i limiti esterni della c.d. materia penale, cioè quando sia possibile attribuire carattere penale ad una sanzione, ai fini dell'applicazione dell'art. 4 del Protocollo 7 della Convenzione Europea dei diritti dell'uomo e dell'art. 6 della Convenzione medesima. Sul punto la Corte di Giustizia di Strasburgo fa costante riferimento ai c.d. criteri elaborati con la sentenza *Engel c. Paesi Bassi* del 8 giugno 1976 e progressivamente affinati.
In estrema sintesi, la Corte ritiene che, al fine di verificare se un procedimento abbia ad oggetto "accuse in materia penale", si dovrebbero considerare tre diversi fattori.
Anzitutto, la qualificazione attribuita dal sistema giuridico nazionale all'illecito contestato; a tale indicazione va però riconosciuto un valore soltanto formale e relativo poiché la Corte deve supervisionare sulla correttezza di tale qualificazione alla luce degli altri fattori indicativi del carattere "penale" dell'accusa.
In seconda istanza, infatti, va considerata la natura sostanziale dell'illecito commesso vale a dire se si è di fronte ad una condotta in violazione di una norma che protegge il funzionamento di una determinata formazione sociale o se è invece preposta alla tutela *erga omnes* di beni giuridici della collettività, anche alla luce del denominatore comune delle rispettive legislazioni dei diversi Stati contraenti.

delinearsi un diritto sanzionatorio di natura marcatamente penalistica, quand'anche il legislatore lo configurasse attraverso illeciti formalmente amministrativi. La Corte EDU è infatti ferma nel ritenere che il carattere penale di un procedimento è subordinato al grado di gravità della sanzione di cui è *a priori* passibile la persona interessata, a prescindere dalla gravità della sanzione in concreto irrogata[31].

Da altro punto di vista, l'imposizione di obblighi di *compliance*[32] nel settore della sicurezza informatica – non diversamente da quanto si è detto a proposito delle fonti di autoregolazione – riverbera i propri effetti sull'estensione di concetti generali del diritto penale, quali ad esempio la colpa specifica, la posizione di garanzia, la prevenibilità dell'evento dannoso, l'agevolazione della condotta illecita altrui. In tal senso, la regolazione della *cybersecurity* è in grado di esercitare un'efficacia indiretta sul raggio d'azione del diritto penale.

Per concludere, sembra che l'intero sistema di *cybersecurity* ruoti attorno a tre fattori: l'importanza delle fonti autoregolamentari, l'individuazione delle fonti di rischio, e l'adozione di misure tecniche e organizzative adeguate a far fronte al rischio individuato. Tali elementi caratterizzanti richiamano alla mente i

---

Infine si deve considerare il grado di severità della pena comminata al responsabile, poiché in una società di diritto appartengono alla sfera "penale" tutte quelle sanzioni che incidono in modo significativo sull'esercizio di diritti e libertà fondamentali.
La CEDU ritiene, dunque, che si debba considerare di natura penale la sanzione che sia qualificata tale dalla norma che la prevede e che, in mancanza, si debba tener conto della natura della violazione o della natura, scopo e gravità della sanzione. In argomento, *ex plurimis* CEDU sent. causa C-199/92 del 1999 *Huls c. Commissione*; sentenza 21 febbraio 1984 *Ozturk c. Germania*, serie A n. 73, par.53; più di recente, in materia di illeciti di *market abuse*, la celebre sentenza *Grande Stevens c. Italia* del 4 marzo 2014 (ric. 2010 n. 18640, 18647, 18663, 18668 e 18698) in *Dir. Pen. Cont*., 9 marzo 2014; da ultimo, in materia di illeciti tributari la sentenza 18 maggio 2017*, Jóhannesson e a. c. Islanda*, (ric. n. 22007/11), in *Dir. Pen. Cont*., 22 maggio 2017.
31 In questo senso la sentenza *Grande Stevens c. Italia, cit*., § 98 nel richiamare la precedente *Engel c. Paesi Bassi, cit.*, § 82. Ancor più di recente, con riferimento alla disciplina sanzionatoria tributaria, si vedano le conclusioni rassegnate lo scorso 12 settembre dall'Avvocato Generale della Corte di Giustizia nella Causa C-524/15 *Menci e altri,* disponibili, con traduzione in lingua italiana, sul sito internet istituzionale della Corte di Giustizia nella sezione dedicata alla ricerca sulle pronunce:
http://curia.europa.eu/juris/recherche.jsf?language=it
32 Intesi quale necessità, per gli operatori qualificati, di adottare *«misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi»* e *«misure adeguate per prevenire e minimizzare l'impatto di incidenti»* (art. 14 della Direttiva NIS).

principi giuseconomici del *risk management* e *assessment*, spesso richiamati con riferimento al sistema di responsabilità degli enti *ex* D. Lgs. 231/2001.

De iure condendo sarebbe opportuno che il sistema evolvesse verso una maggiore responsabilizzazione della sfera collettiva, e che l'apparato sanzionatorio – sia esso penale o amministrativo – fosse modellato attorno alla persona giuridica, anziché quella fisica. Del resto, le figure soggettive gravate dagli obblighi di sicurezza (operatori dei servizi essenziali, fornitori di servizi digitali) si identificano in realtà societarie estremamente articolate e complesse, il che renderebbe inopportuno l'introduzione di forme di responsabilità (soltanto) individuale.

5. Conclusioni. Il panorama normativo attuale non consente di affermare l'esistenza di un diritto penale della sicurezza informatica e della protezione cibernetica. Si tratta di una materia che, fino ad oggi, si è evoluta in seno alle organizzazioni complesse attraverso le fonti di autoregolazione.

Tuttavia, il ruolo della *compliance* nel governo del cyber-rischio si palesa di fondamentale importanza e, talvolta, incide sul *range* d'azione del diritto penale: può infatti accadere che il precetto di alcune fattispecie di reato si presti ad essere riempito di contenuto attraverso il richiamo implicito alle disposizioni autoregolamentari o che l'estensione di alcune clausole generali o elastiche vada parametrato a quest'ultime.

Con la Direttiva NIS il legislatore europeo ha riaffermato, a livello positivo, la centralità dell'adozione di piani, strategie e misure di *governance* del rischio cyber non solo a livello di politica nazionale, ma soprattutto per gli operatori dei servizi essenziali e i fornitori di servizi digitali. In prospettiva futura, quindi, ci si attende che il diritto sanzionatorio evolva nel senso di una radicale responsabilizzazione delle persone giuridiche per l'omessa adozione delle misure tecniche e organizzative idonee a prevenire e minimizzare l'impatto delle minacce del cyberspazio.

Il futuro, dunque, vede la *compliance* come fattore di garanzia della sicurezza dei dati e della protezione delle informazioni. Che sia proprio questa

– per tornare alla metafora d'apertura – la *longa manus* dello Stato, l'arma mitologica "capace di offendere e guarire", pur di preservare la libertà di *internet*?

Riferimenti bibliografici

ANTOLISEI F., *Manuale di diritto penale. Parte speciale*. Vol.II, Milano, 2008, p. 395
BONAFEDE M, *L'accertamento della colpa specifica,* Padova, 2005, p. 62
BOSI G., *Autoregolazione societaria*, Milano, 2009, p. 109 ss.
CARCATERRA G., *Presupposti e strumenti della scienza giuridica,* Torino, 2011, p. 3
CASTRONUOVO D., *Clausole generali e diritto penale*, in *Dir. Pen. Cont*., 14 novembre 2012, p. 3 ss
CASTRONUOVO D., *La colpa penale*, Milano, 2009 p. 130 ss
CUOMO L., IZZI B., *Misure di sicurezza e accesso abusivo ad un sistema informatico o telematico*), in *Cass. Pen*. 2002, p. 1015
DE BENEDETTO M., *L'organizzazione della funzione di regolazione*, in *Studi parlamentari e di politica costituzionale*, 2005, fasc. 149-150, p. 73 ss
FERRETTI A., *Irrilevante per la configurazione del reato di accesso abusivo in un sistema informatico la finalità che ha motivato l'ingresso*, in *Diritto & Giustizia*, fasc. 30, 2015, p. 81 ss
FIANDACA G. MUSCO E., *Diritto Penale. Parte speciale*., vol. I, Milano, 2012, p. 264
FLICK G.M., NAPOLEONI V., *A un anno di distanza dall'"Affaire Grande Stevens": dal "bis in idem" all'"e pluribus unum"?* in *Rivista AIC*, 2015, fasc. 3, pp. 34;
FORTI G., *Colpa ed evento nel diritto penale*, Milano, 1990 p. 309
MAGGI B., *De l'agir organisationnel: un point de vue sur le travail, le bien-être, l'apprentissage*, Toulouse, 2003, p. 25
MANTOVANI F., *Principi di diritto penale*, Padova, 2002 p. 3 ss.
MARANI S., *Principio di determinatezza e norma integratrice del precetto penale*, Firenze, 2014 p. 32
PALAZZO F., *Introduzione ai principi del diritto penale*, Torino, 1999, p. 199 ss;
PECORELLA C., *L'attesa pronuncia delle Sezioni unite sull'accesso abusivo a un sistema informatico: un passo avanti non risolutivo,* in *Cass. Pen*. 2012, 11, p. 3681 ss.
PICOTTI L., *Diritti fondamentali nell'uso e nell'abuso dei social network. Aspetti penali.*, in *Giur. mer*., 2012, 12, p. 2523
RISICATO L., *Gli elementi normativi della fattispecie penale*, Milano, 2004, p. 197
RODOTÀ S., *Una Costituzione per Internet*, in *Pol. dir*. 2010, 3, p. 339
ROMANO M., *Commentario sistematico al codice penale. I delitti contro la pubblica amministrazione. I delitti dei pubblici ufficiali*, Milano, 2013, p. 307;
SCAROINA E., *Costi e benefici del dialogo tra corti in materia penale. La giurisprudenza nazionale in cammino dopo la sentenza Grande Stevens tra disorientamento e riscoperta dei diritti fondamentali*, in *Cass. Pen*., 2015, fasc. 7-8, pp. 2910-2943.
SEVERINO P., *Le frontiere della sicurezza informatica e prevenzione del cybercrime*, in *Luiss Open,* 8 settembre 2017 p. 8 ss.;
TRIPODI A. F., *Uno più uno (a Strasburgo) fa due. L'Italia condannata per violazione del ne bis in idem in tema di manipolazione del mercato*) in *Dir. Pen. Cont*., 9 marzo 2014
VIGANÒ F., *Una nuova sentenza di Strasburgo su ne bis in idem e reati tributari*, in *Dir. Pen. Cont*., 22 maggio 2017
ZANIER M.L., *L'accusa penale in prospettiva socio-giuridica*, Milano 2012 p. 28
ZICCARDI G., *Cyber Law in Italy*, 2011, NL, p. 15 ss