Issn: 2612-4491

Diritto di INTERNET

Digital Copyright e Data Protection

RIVISTA TRIMESTRALE

2020
1

IN EVIDENZA

- Perimetro di Sicurezza Nazionale Cibernetica
- Esecuzione di un ordine di acquisto via internet
- Quantificazione del danno da diffamazione online
- Pluralismo politico online. La vicenda Casapound
- Revoca del consenso per la pubblicazione di immagini su Facebook
- Adwords e concorrenza sleale
- Sulla ricondivisione degli hashtag "vietati"
- Falso curriculum su Linkedin
- Web harvesting, banche dati e Antitrust
- Clausola vessatoria su Booking
- Riconoscimento fotografico mediante immagine tratta da un social network
- Hackeraggio etico
- Foto acquisite tramite Google Earth e valore probatorio
- Financial Cybercrime
- Guerre cibernetiche

Pacini Giuridica

SOMMARIO

SAGGI

IL SIGNIFICATO DI PERSONA, AI TEMPI DI INTERNET
di Renato Clarizia 3

CYBERSECURITY: QUID NOVI?
di Lorenzo Picotti 11

IL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA
di Stefano Mele 15

GIURISPRUDENZA

EUROPEA

RIGHT TO BE FORGOTTEN ONLINE E IL DISCUTIBILE RUOLO DEI GESTORI DEI MOTORI DI RICERCA 27
Corte di Giustizia UE (grande sezione); sentenza 24 settembre 2019; causa C - 507/17
Corte di Giustizia UE (grande sezione); sentenza 24 settembre 2019; causa C - 136/17
commento di Maria Astone 28

CIVILE

LA NATURA IMPERATIVA DEI PRINCIPI DI PROTEZIONE DEI DATI PERSONALI: CONSEGUENZE IN AMBITO BANCARIO 35
Corte di Cassazione; sezione I civile; ordinanza 21 ottobre 2019, n. 26778
commento di Giulia Fatano 38

ORDINE DI INVESTIMENTO *ON-LINE* OLTRE IL LIMITE DI PROVVISTA E RESPONSABILITÀ DELL'INTERMEDIARIO 45
Corte di Cassazione; sezione VI civile; ordinanza 15 ottobre 2019, n. 26077
commento di Ludovica Molinario 46

APPLICAZIONE DEI PARAMETRI ADOTTATI DALLE TABELLE DI MILANO PER IL RISARCIMENTO DEL DANNO DA DIFFAMAZIONE TRAMITE *FACEBOOK* 53
Corte d'Appello dell'Aquila; sezione civile; sentenza 13 novembre 2019, n. 1888
commento di Sabrina Peron 56

PLURALISMO POLITICO E DIBATTITO PUBBLICO ALLA PROVA DEI *SOCIAL NETWORK* 63
Tribunale di Roma; sez. spec. imprese; ordinanza 12 dicembre 2019 n. 59264
commento di Andrea Venanzoni 65

ADWORDS E CONCORRENZA SLEALE 73
Tribunale di Milano; sez. spec. imprese; sentenza 8 novembre 2019, n. 10130
commento di Alessandro La Rosa 79

CONSENSO E TUTELA DEL DIRITTO ALL'IMMAGINE DEL MINORE: TRA DIRITTO DELLA PERSONALITÀ E PROTEZIONE DEI DATI PERSONALI 87
Tribunale di Bari; sezione II civile; ordinanza 7 novembre 2019
commento di Michela Maggi 88

SIGARETTE ELETTRONICHE, PUBBLICITÀ *ONLINE* E LICEITÀ DELLA RICONDIVISIONE DEI C.D. *USER GENERATED CONTENTS* "VIETATI" 93
Tribunale di Roma; sez. spec. imprese; ordinanza 5 novembre 2019
commento di Michele Papa 98

SELEZIONE PER IL RECLUTAMENTO DEL PERSONALE DELLE SOCIETÀ PUBBLICHE E FALSO *CURRICULUM* SU *LINKEDIN* 105
Tribunale di Trapani; sezione lavoro; sentenza 2 ottobre 2019, n. 522
commento di Claudia Serrapica 108

WEB HARVESTING, SCRAPING OR DATA EXTRACTION, TUTELA DELLE BANCHE DATI SECONDO LA LEGGE SUL DIRITTO D'AUTORE E PRINCIPI DI DIRITTO ANTITRUST 113
Tribunale di Roma; sez. spec. imprese; ordinanza 5 settembre 2019, n. 34006
commento di Bruno Tassone e Marco Barbone 117

DISDETTA ALBERGHIERA E CLAUSOLA VESSATORIA SU *BOOKING* 127
Giudice di Pace di Trapani; sezione civile; sentenza 14 ottobre 2019
commento di Alessandro Torroni 127

PENALE

DELLA RILEVANZA PENALE DELLA CREAZIONE ABUSIVA DELL'*ACCOUNT* E DEL SUCCESSIVO INSERIMENTO DI DATI PERSONALI ALTRUI SU UN *SOCIAL NETWORK* 135
Corte di Cassazione; sezione III penale; sentenza 17 ottobre 2019, n. 42565
commento di Andrea De Lia 137

LA "DEBOLE" RILEVANZA PENALE DELLO SPAMMING, TRA CONSENSO IMPLICITO AL TRATTAMENTO E INSUSSISTENZA DEL NOCUMENTO 143
Corte di Cassazione; sezione III penale; sentenza 10 ottobre 2019, n. 41604
commento di Pasqualino Silvestre 146

"RICOGNIZIONI INFORMALI 2.0": IL RICONOSCIMENTO FOTOGRAFICO MEDIANTE IMMAGINE TRATTA DA UN *SOCIAL NETWORK* 155
Corte di Cassazione; sezione II penale; sentenza 12 settembre 2019, n. 42315
commento di Federica Centorame 157

IL DIRITTO PENALE ALLA PROVA DELL'*HANDS-ON* DELL'*ETHICAL HACKING* 165
Tribunale di Catania; giudice per le indagini preliminari; decreto di archiviazione 15 luglio 2019
commento di Roberto Flor 165

AMMINISTRATIVA

VALORE PROBATORIO DELLE FOTO ACQUISITE TRAMITE *GOOGLE EARTH* 171
T.a.r. Sardegna; sez. I; sentenza 8 ottobre 2019, n. 779
commento di Francesco d'Amora 173

LA SEDUCENTE PERFEZIONE DI ALGORITMI E INTELLIGENZA ARTIFICIALE NELLE PROCEDURE AMMINISTRATIVE ALLA LUCE DEI MODELLI DI RESPONSABILITÀ CIVILE 177
T.a.r. Lazio-Roma; sezione III Bis; sentenza 13 settembre 2019, n. 10964
commento di Mariangela Ferrari 178

PRASSI

LE GUERRE CIBERNETICHE TRA RISCHI E DETERRENZA
di Gabriele Suffia 187

IL *FINANCIAL CYBERCRIME* NELLA PROSPETTIVA DELLA V DIRETTIVA EUROPEA ANTIRICICLAGGIO (843/2018/UE)
di Ramona Barbabietola 195

Cybersecurity: quid novi?

di Lorenzo Picotti

Sommario: 1. La "sicurezza informatica" come nuovo bene giuridico. – 2. Il passaggio dai *computer crime* ai *cybercrime* e l'armonizzazione sovranazionale. – 3. Nuove frontiere della "sicurezza cibernetica" (*cybersecurity*). – 4. Conclusioni.

Il saggio tratta dell'evoluzione della "sicurezza informatica", che segue la trasformazione del *web* in un *Cyberspace* globale, in cui le nuove minacce, anche a diritti ed interessi fondamentali della persona e della collettività, richiedono risposte adeguate, come dimostra già il passaggio dalla ristretta categoria dei *computer crime* a quella ben più estesa dei *cybercrime*, riflessa nei corrispondenti interventi di armonizzazione sovranazionale. Oggi la nuova "sicurezza cibernetica" *(cybersecurity)* non è più affidata solo ai singoli titolari dei sistemi, ma è demandata a penetranti poteri delle autorità pubbliche, come ben si evince dalle norme europee e nazionali più recenti, come quelle sul "Perimetro di Sicurezza Nazionale Cibernetica" (d.l. 105/2019, conv. in l. 133/2019).

The Paper deals with the evolution of cybersecurity within that of Cyberspace and the harmonization rules for cybercrime. Overcoming the idea that only the titular of each Information-system was responsible for his security, the recent European and national sources and in particular the legislative decree 105/2019 conv. by law 133/ 2019, containing "urgent provisions" on the "National Cyber Security Perimeter", intends ensure a "high level of security of networks, information systems and IT services" giving broad powers to the public authorities. The Paper deals with the problem of the provision of harmonization rules for cybercrime, with particular reference to the legislative decree September 21, 2019, n. 105, conv. with amendments by law 18 November 2019 n. 133, containing "urgent provisions" on the "National Cyber Security Perimeter", which intends to ensure a "high level of security of networks, information systems and IT services".

1. La "sicurezza informatica" come nuovo bene giuridico

Di "sicurezza informatica" come nuovo bene giuridico, nato dallo sviluppo dei sistemi informatici e telematici e dalla loro crescente diffusione nelle strutture pubbliche e private, si è cominciato a parlare in Italia dalla fine degli anni Ottanta, quando è emersa, con la loro vulnerabilità, la necessità di affiancare alle misure di sicurezza tecniche, anche presidi di natura giuridico-penale, per prevenire e reprimere condotte offensive di dati, programmi, sistemi. L'ottica era sostanzialmente quella di una protezione contro le minacce dei c.d. *computer crime*, che crescevano parallelamente all'informatizzazione di settori sempre più importanti dell'economia e della pubblica amministrazione, da quello bancario ed assicurativo, fino alla sanità ed alla finanza, in modo da colpire anche penalmente le aggressioni alla riservatezza, all'integrità, alla disponibilità dei dati, delle informazioni e dei sistemi stessi. In altri termini, la sicurezza informatica era vista come *strumentale* alla tutela di altri beni giuridici "finali", sia della persona, sia della collettività (1).

Da un lato, quindi, si riconducevano ad essa le nuove fattispecie incriminatrici dei danneggiamenti informatici (vale a dire di dati, programmi e sistemi informatici: nel nostro ordinamento sanzionati dagli art. 420 e 635-*bis* c.p., quali rispettivamente modificato ed introdotto dalla legge 23 dicembre 1993, n. 547, la prima contro la criminalità informatica, poi trasfusi, con modificazioni, negli articoli da 635-*bis* a 635-*quinquies* c.p. ad opera della legge 18 marzo 2008, n. 48, di attuazione della Convenzione *Cybercrime* di cui si dirà), colpendo anche condotte prodromiche, quali il procurarsi ed il diffondere programmi *virus* con lo scopo di danneggiare sistemi, informazioni, dati o programmi (art. 615-*quinquies* c.p. introdotto dalla legge 547/1993 e riformulato dalla legge 48/2008)(2); dall'altro si sanzionavano penalmente le aggressioni alla "riservatezza informatica", quale bene giuridico parimenti nuovo, nato con lo sviluppo tecnologico, e corrispondente al diritto di escludere terzi da propri spazi informatici riservati o, come si diceva, dal proprio "domicilio informatico", colpendo l'accesso abusivo ad un sistema altrui, nonché la condotta prodromica di detenere o diffondere abusivamente codici, parole chiavi o altri mezzi di accesso (artt. 615-*ter* e 615-*quater* c.p., introdotti dalla legge 547/1993)(3).

(1) Al riguardo sia consentito rinviare a PICOTTI, *Sicurezza, informatica e diritto penale*, in DONINI, PAVARINI (cur.), *Sicurezza e diritto penale*, Bologna 2011, 217 s.

(2) Per un quadro in argomento cfr. SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, in *Riv. it. dir. proc. pen.*, 2012, 204 s.

(3) Sulla distinzione fra "riservatezza informatica", che trova tutela penale nel codice fra i delitti contro la persona, e disciplina anche sanzionatoria, non solo penale, dei dati personali, contenuta nel Codice privacy (ed oggi soprattutto nel Regolamento dell'Unione europea 2016/679:

La tutela penale peraltro era (come ancor oggi) subordinata all'*onere* di proteggere i sistemi stessi con "misure di sicurezza", in conformità al principio di *extrema ratio* della sanzione penale ed in conformità alla concezione privatistica della sicurezza stessa, quale bene sostanzialmente disponibile in capo al titolare del sistema informatico (4).
Per vero la nuova disciplina sulla raccolta ed il trattamento dei dati personali, vale a dire della *privacy* strettamente intesa, di cui alla legge 31 dicembre 1996, n. 675, presidiava penalmente l'*obbligo* di garantire, da parte del titolare del trattamento, la "sicurezza dei dati personali", che potevano essere di terzi, adottando le "misure di sicurezza necessarie" quali prescritte da appositi decreti ministeriali previsti dall'art. 15, tanto da punirne l'omissione anche solo colposa (art. 36). Presidio penale sostanzialmente riprodotto nell'art. 169 del Codice privacy di cui al d.lgs. 30 giugno 2003, n. 196, che pur articolava in termini più ampi ed elastici l'obbligo della sicurezza, sanzionando penalmente la mancata adozione – seppur sempre anche solo colposa – delle "misure minime" di cui all'art. 31. Tali norme sono però state abrogate dal d.lgs. 10 agosto 2018, n. 105, di adeguamento del Codice privacy al Regolamento generale dell'Unione europea 2016/679 in materia di trattamento dei dati personali (c.d. GDPR), che ha affidato ad una diversa disciplina dinamica, basata sulla valutazione e prevenzione dei rischi specifici per i diversi trattamenti e dati che vengano in rilievo, ed a sanzioni amministrative assai incisive, la tutela della sicurezza in tale campo (5).

2. Il passaggio dai *computer crime* ai *cybercrime* e le norme di armonizzazione sovranazionale

Se è emersa, quindi, l'esigenza che la "sicurezza" perlomeno nel trattamento dei dati personali si configurasse come *obbligo*, penalmente e comunque fortemente sanzionato, e non più quale mero *onere* per la tutela penale della "propria" sfera di riservatezza informatica, stante l'evidente stretta connessione fra i due beni, il passaggio epocale è stato segnato dalla dimensione pervasiva e dal ruolo essenziale che ha assunto la rete globale, o meglio il *Cyberspace*, quale realtà non solo tecnologica, ma di assorbente interazione, scambio e comunicazione permanente, fra qualsivoglia soggetto ed ente, pubblico e privato, in cui la sicurezza – divenuta "cibernetica" – è assurta ad interesse primario e per certi aspetti totalizzante, non solo della persona, ma anche o prima di tutto della collettività.
Non si tratta infatti più solo di fronteggiare nuove tipologie di singole condotte, penalmente illecite, definite oggi quali *cybercrime*, perché costituite da ogni genere di delitti – non solo quelli informatici strettamente intesi – che si possono realizzare in rete (o meglio nel *Cyberspace*) (6): dall'estorsione, al riciclaggio (7), dalle truffe e frodi nei mezzi di pagamento, al *cyberstalking* e *cyberbullismo*, fino ai più gravi attacchi del *cyberterrorism*, se non anche del *cyberwarfare*.
Contro le offese più tradizionali sono stati e vengono certamente adeguati gli strumenti del diritto penale e del diritto processuale penale, come ben dimostra la lungimirante Convenzione *Cybercrime* adottata fin dal 2001 dal Consiglio d'Europa (8). In essa, accanto alla previsione di norme d'armonizzazione dei crimini informatici, offensivi della classica triade di beni giuridici rappresentati dalla confidenzialità, integrità e disponibilità dei dati e dei sistemi informatici (ripresi anche nella Direttiva UE 2013/40), oltre che di altri delitti cibernetici quali la pedopornografia e le più gravi violazioni dei diritti d'autore, sono state stabilite essenziali norme di adeguamento ed armonizzazione della disciplina processuale in materia di ricerca, raccolta, conservazione ed utilizzazione delle *prove elettroniche*, riguardanti *qualsivoglia reato* (art. 14, par. 2, lett. c), non solo commesso in rete o tramite mezzi informatici, al fine di garantire la massima assistenza reciproca e cooperazione internazionale fra gli Stati parte (artt. 27 segg.) nella repressione della criminalità che si realizzi o manifesti in ogni sua possibile forma nella rete.

c.d. GDPR), sia consentito rinviare a PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in ID. (cur.), *Tutela penale della persona e nuove tecnologie*, Padova 2013, 59 s.

(4) Si vedano in specie FLOR, *Verso una rivalutazione dell'art. 615* ter *c.p.? Il reato di accesso abusivo a sistemi informatici o telematici fra la tutela di tradizionali e di nuovi diritti fondamentali nell'era di Internet*, in <www.penalecontemporaneo.it> (2.5.2012); SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in PICOTTI (cur.), *Tutela penale della persona*, cit., 125 s.

(5) Un primo quadro è stato offerto da FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna 2017.

(6) Per la distinzione fra le diverse categorie di reati commessi in rete in un quadro sistematico cfr. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (cur.), *Cybercrime*, Milano 2019, 33 s.

(7) In argomento volendo PICOTTI, *Profili penali del* Cyberlaundering: *le nuove tecniche di riciclaggio*, in *Riv. trim. dir. pen. ec.*, 2018, 560 s., nonché SOANA, *Cripto-valute e riciclaggio. Modus operandi e tentativi regolatori*, in questa ***Rivista***, 2019, 671.

(8) Sul punto volendo PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008 n. 6, 700 s.; in generale cfr. CORASANITI, CORRIAS LUCENTE (cur.), *Cybercrime, responsabilità degli enti, prova digitale. Commento alla Legge 18 marzo 2008, n. 48*, Padova, 2009; LUPARIA (cur.), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest*, Milano 2009.

3. Nuove frontiere della "sicurezza cibernetica" (*cybersecurity*)

Ma oggi la "sicurezza cibernetica" (*cybersecurity*) ha assunto un'importanza ed una dimensione ancor più ampie e pervasive, che si manifestano in un approccio anche giuridico radicalmente diverso (9).

Si deve infatti muovere dal riconoscimento che dalle reti e dai sistemi informatici dipendono ormai funzioni e servizi *essenziali*, per la società, l'economia, i diritti e gli interessi pubblici e privati.

L'approccio è quindi quello di assicurare, a livello generale, un elevato grado di sicurezza delle reti e dei sistemi *in quanto tali*, avendo essi stessi acquisito il rango di autonomi "beni giuridici", in determinati contesti, con meccanismi quindi di "mappatura" delle infrastrutture critiche, determinazione di regole dinamiche di prevenzione e *compliance*, segnalazione obbligatoria di attacchi ed incidenti che mettano *a rischio* l'esercizio delle funzioni e dei servizi dipendenti da tali reti e sistemi.

Al riguardo basti segnalare la diversa prospettiva adottata, rispetto alla Direttiva comunitaria 95/46, dal citato Regolamento UE 2016/679 (c.d. GDPR), in materia di trattamento e circolazione dei dati personali, per garantire la sicurezza in tale campo, che ormai abbraccia sempre più vaste categorie di dati e sistemi: il titolare del trattamento deve oggi adeguare dinamicamente ad essi il livello di attenzione e responsabilizzazione, secondo parametri generali di valutazione dei rischi, risposta e tracciamento (artt. 33 e 34), per prevenire e contrastare violazioni ed anche eventi accidentali (art. 4), che vanno segnalati e comunicati, nelle condizioni stabilite, anche agli interessati, per evitare più gravi conseguenze ed incidenti futuri. E le violazioni sono come detto punite da severe sanzioni amministrative, stabilite dal Regolamento, che ha efficacia diretta negli Stati membri, oltre che dalle sanzioni penali riformulate a livello nazionale dal d.lgs. 10 agosto 2018, n. 101.

Di grande rilievo è soprattutto la Direttiva UE 2016/1148 sulla sicurezza delle reti e dei sistemi informatici (c.d. NIS) (10), che ha posto le basi di una più efficace cooperazione e capacità di risposta degli Stati membri in materia, stabilendo in particolare obblighi stringenti di valutazione e gestione del rischio in capo agli operatori di servizi essenziali (in particolare nei settori sanitario, bancario, finanziario, dell'energia, del trasporto, dell'acqua potabile), ed ai fornitori di servizi digitali, siano essi pubblici o privati, che devono altresì notificare i più gravi incidenti relativi alla sicurezza alle competenti autorità nazionali (c.d. CSIRT: *Computer Security Incident Report Team*), il cui coordinamento fa poi capo all'ENISA (l'Agenzia europea per la sicurezza informatica), istituita nel 2004 ed i cui compiti si sono via via ampliati, fino a quelli di predisporre gli schemi di certificazione della sicurezza dei prodotti, servizi e processi informatici, previsti dal Regolamento UE 2019/881 (c.d. *Cybersecurity Act*).

In ambito nazionale, accanto alla normativa d'attuazione della Direttiva NIS, in specie ad opera del d.lgs. 18 marzo 2018, n. 65, è da ultimo intervenuto il d.l. 21 settembre 2019, n. 105, conv. con modificazioni dalla legge 18 novembre 2019 n. 133, recante "disposizioni urgenti" in materia di "*Perimetro di Sicurezza Nazionale Cibernetica*" (11) che intende assicurare un "livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici" ben al di là dei settori sopra indicati, applicandosi a tutte le amministrazioni pubbliche, agli enti ed agli operatori pubblici e privati, aventi una sede nel territorio nazionale, "da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale" (12).

Per tale così vasto ambito di soggetti ed attività è introdotta un'articolata disciplina, che definisce in termini generali i soggetti pubblici e privati coinvolti, i vari obblighi ed adempimenti cui sono tenuti, in particolare di predisporre gli elenchi delle reti e l'analisi dei rischi, nonché le misure da adottare per fronteggiarli, sia pure con criteri di gradualità, i poteri di certificazione, controllo, ispezione, prescrizione delle autorità governative, le norme in materia di acquisizione e utilizzazione delle tecnologie rilevanti, e quant'altro, rinviando poi in gran parte le norme primarie ad atti amministrativi che dovranno essere adottati dal Presidente del Consiglio dei Ministri, con il supporto del Comitato Interministeriale

(9) Per una panoramica sul tema v. FLOR, *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in questa ***Rivista***, 2019, 453.

(10) Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. Il testo è disponibile al seguente link <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016L1148>. In Italia, la suddetta Direttiva è stata attuata attraverso il decreto legislativo 18 maggio 2018, n. 65, "Attuazione della Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione". Il testo è disponibile al seguente link <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2018-05-18;65!vig=>.

(11) Il testo è disponibile al seguente link < https://www.gazzettaufficiale.it/eli/id/2019/11/20/19G00140/sg>. Legge 18 novembre 2019, n. 133, "Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica".

(12) Cfr. sul punto l'esaustivo quadro offerto da MELE, *Il Perimetro di Sicurezza Nazionale Cibernetica*, in questa ***Rivista***, 2020, 15 s.

per la Sicurezza della Repubblica (CISR), entri termini prefissati (già oggetto di modifiche ad opera del d.l. 30 dicembre 2019, n. 162, c.d. milleproroghe, in corso di conversione).
Nella sua architettura complessiva, il sistema prevede una competenza regolatoria della Presidenza del Consiglio nei confronti dei soggetti pubblici, nonché di soggetti che forniscano "servizi fiduciari qualificati", di posta elettronica, di gestione dell'identità digitale, di conservatore di documenti informatici; e del Ministero dello Sviluppo Economico nei confronti degli altri soggetti privati. Per cui rispettivamente all'una o all'altro andranno indirizzati gli adempimenti degli obblighi di comunicazione, di notifica di incidenti rilevanti, di adozione delle misure di sicurezza e quant'altro previsto dalla nuova disciplina, di cui è importante sottolineare anche il ruolo attribuito al Centro di Valutazione e Certificazione Nazionale (CVCN), in particolare per elaborare le misure di sicurezza e le metodologie di verifica e valutazione del rischio, che si raccorderà come organo tecnico alle funzioni demandate dal *Cybersecurity Act* europeo sopra menzionato.
Resta da aggiungere che la nuova normativa in materia di "*Perimetro di Sicurezza Cibernetica Nazionale*" è intervenuta, ampliandola ad ulteriori casi e situazioni, anche sulla disciplina dei c.d. *Golden Power*, ossia dei poteri speciali attribuiti al Governo in settori che toccano in generale la difesa e la sicurezza nazionali (d.l. 15 marzo 2012, n. 21 e successive modifiche, in specie ad opera del d.l. 25 marzo 2019, n. 22, conv. dalla legge 20 maggio 2019, n. 41, in materia di reti di telecomunicazione elettronica a banda larga con tecnologia 5G), in forza dei quali esso ha poteri di veto, di imporre condizioni, di opporsi all'acquisto di partecipazioni societarie da parte di soggetti esterni all'Unione europea, che possano compromettere gli interessi della difesa e della sicurezza nazionale (13).

4. Conclusioni

Dunque, può concludersi che il tema della "sicurezza", prima *informatica*, ora *cibernetica*, è divenuto, da ambito privato e disponibile, passando ad obbligo di natura pubblica variamente articolato a seconda dei settori di interesse, le cui violazioni sono state anche penalmente sanzionate, un terreno oggi vastissimo e fondamentale, particolarmente sensibile all'esercizio dell'attività di alta amministrazione, se non della politica, interna ed estera, oltreché economica.
Tale marcata evoluzione riflette certamente il parallelo pervasivo sviluppo del *Cyberspace*, che ha finito per assorbire o comunque intrecciarsi indistricabilmente con ogni dimensione della società odierna, compresa quella amministrativa, economica, politica.
Il rischio, tuttavia, è evidente, se non c'è il parallelo presidio, attento ed efficace, di una legittimazione e di un controllo democratici e trasparenti, che nell'indefinito campo delle categorie "aperte" della sicurezza e della difesa nazionale, sappiano garantire il nucleo essenziale del rispetto dei diritti e delle libertà fondamentali delle persone, a partire dalle libertà economiche, di espressione, di informazione, di accesso alla rete, che fanno capo a ciascuno, persona fisica od ente.
La sicurezza cibernetica è oggi, certamente, la condizione per l'esercizio anche di questi diritti, oltre che dei servizi e delle funzioni essenziali nella società globale. E tutti i soggetti coinvolti devono (poter) parteciparvi. Ma proprio per questo, il ruolo del diritto penale non può essere relegato al ruolo "meramente sanzionatorio" di punire (con la reclusione da 1 a 3 anni) le più diverse violazioni della disciplina extrapenale, in gran parte stabilita a livello amministrativo, secondo la tecnica della norma penale in bianco, come è sostanzialmente quella di cui all'art. 1, comma 11, del d.l. 105/2019: delitto che a sua volta rientra ora, quale reato presupposto, nella sfera di responsabilità degli enti, ai sensi del d.lgs. 8 giugno 2001, n. 231, il cui art. 24-*bis* è stato a tal fine esteso, accanto ad un complesso di sanzioni amministrative assai incisive, previste dal comma 9 dell'art. 1 citato, non solo di natura pecuniaria (varianti fra minimi da 200.000 a 300.000 Euro e massimi da 1.200.000 e 1.800.000 Euro), ma anche di natura interdittiva.
Infatti, nel quadro strategico, non solo europeo, che mira a rafforzare incisivamente e strutturalmente la tutela della *cybersecurity*, i così penetranti poteri preventivi, prescrittivi e sanzionatori delle Autorità governative dovranno essere accompagnati dal contrappeso di una forte vigilanza, prevenzione e se del caso repressione di qualsiasi abuso, uso improprio o anche solo strumentale di quei poteri e dell'ampia sfera di discrezionalità che vi è connessa, al fine di salvaguardare le condizioni basilari dello Stato democratico di diritto, che non può divenire esso stesso vittima delle minacce alla sicurezza cibernetica.

(13) Cfr. sul punto ancora MELE, *Il Perimetro*, cit., 20 s.