PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA, DAL D.L. 105/2019 AI D.P.C.M. N. 131/2020 E N. 81/2021: LA SUBLIMAZIONE DELLE CC.DD. *INFORMATION AND COMMUNICATION TECHNOLOGIES.*

Fabio Carchidi

Abstract: (ITA)
Si discorre, nei termini della riservatezza quale estrinsecazione del principio solidaristico dell'ordinamento, sui prodromi di una vera e propria rivoluzione copernicana sul tema della cybersicurezza, infatti, il perimetro di sicurezza nazionale cibernetica, incardinato dal D.l. 105/2019, garantisce la sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato; tutto ciò detto, all'interno di un progresso esponenziale in materia di Information e Communication Technologies porta alla sublimazione, in subjecta materia, dei principi contemplati nel Regolamento 2016/679, nel caso di specie la c.d. privacy by design, postulata dai proposti meccanismi di certificazione.

Abstract: (ENG)
In terms of confidentiality as an expression of the principle of solidarity of the system, the prodromes of a true Copernican revolution on the subject of cybersecurity are discussed, in fact, the perimeter of national cyber security, hinged by the Legislative Decree 105/2019, guarantees the security of networks, information systems and computer services of public administrations of public and private entities and operators with a headquarters in the national territory, on which depends an essential function of the State. 105/2019, guarantees the security of networks, information systems and computer services of public administrations of public and private entities and operators located in the national territory, on which depends the exercise of an essential function of the State; all this said, within an exponential progress in the field of Information and Communication Technologies leads to the sublimation, in subjecta materia, of the principles laid down in Regulation 2016/679, in this case the so-called privacy by design, postulated by the proposed certification mechanisms.

SOMMARIO: 1. Quadro normativo in materia di sicurezza cibernetica. Dall'allegato B del D.lgs 196/2003 alla prospettiva europea del Regolamento UE n. 881/2019; **1.2** L'impatto dell'ENISA sui sistemi di certificazione. Postulare la c.d. *privacy by design*; **2.** Il perimetro di sicurezza nazionale cibernetica. Premesse del formante legislativo; **2.1** Fenomenologia applicativa del Perimetro di Sicurezza Nazionale Cibernetica: i D.P.C.M.; **3.** ICT *practices and career development*. Il caso e- portfolio. Il surplus dell'uomo-macchinico.

1. Quadro normativo in materia di sicurezza cibernetica. Dall'allegato B del D.lgs 196/2003 alla prospettiva europea del Regolamento UE n. 881/2019.

Il formante legislativo italiano non prevedeva, fino a poco tempo fa, normative concrete in materia di cybersicurezza, infatti, l'orizzonte interpretativo si rifaceva pedissequamente al c.d. "*Disciplinare tecnico in materia di misure minime di sicurezza*" nell'Allegato B al D.lgs. 196/2003; invero, il D.lgs. 101/2018, nel conformare il D.lgs. 196/2003 alle disposizioni del RGPD, ha tenuto conto della particolare circostanza secondo la quale un approccio al tema della protezione dei dati, soprattutto nell'ambito della sicurezza informatica, è in progressiva evoluzione e in virtù del *considerando 6* dello stesso Regolamento, non può esimersi dall'adattamento alla realtà circostante.

Tant'è che è soltanto dalla seconda metà del 2019 che il quadro legislativo comunitario e nazionale ha assunto elevata concretezza: dalla prospettiva europea con il Regolamento UE n. 881/19, entrato in vigore alla fine di giugno 2019, e dal punto prospettivo nazionale con il decreto-legge n. 105 del 2019, convertito in legge nel novembre 2019 e poi modificato nel febbraio 2020 [1].

1 Per ulteriori informazioni sul complesso tema delle fonti in materia di cybersicurezza v. B. BRUNO, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali,* in *Federalismi,* n. 14/2020, ISSN: 18263534; pp. 12-15 nel quale l'autore espone un allineamento teorico e sincronico del formante legislativo nazionale e comunitario; si veda anche il REG. UE 2016/679, in specifico al *Considerando n. 6*: «*La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di*

In siffatto contesto è lapalissiana la *compliance* della normativa - sinora citata- alla *Direttiva NIS* dell'UE [2] in qualità di una cornice sovranazionale volta a stabilire i principi cardine per il conseguimento di un livello di sicurezza della rete e dei sistemi informativi per una ragione tutelata sia a livello nazionale, nell'articolo 41 della Costituzione Repubblicana[3] che il Togliatti definisce compromesso, sia a livello sovranazionale in quanto la Corte del Lussemburgo dichiara di «*aver sacrificato il valore della concorrenza dell'Unione in favore dell'utilità sociale del diritto al lavoro*»[4].

Ai fini espositivi è utile rammentare gli agenti destinatari delle normative comunitarie in tale assetto, ovverosia gli operatori di servizi essenziali *rectius* soggetti pubblici e privati che erogano servizi nel settore sanitario, bancario, dell'energia, del trasporto, della fornitura e distribuzione di acqua potabile, delle infrastrutture dei mercati finanziari e delle infrastrutture digitali, ma soprattutto dei *servizi digitali,* che elargiscono varie tipologie di servizi online (e.g motori di ricerca online e *cloud computing*). [5]

I succitati atti normativi (n.d.r. D.l. 105/2019 e Reg. 881/19) non presentano riferimenti sinallagmatici al loro interno, tuttavia, l'incrocio di norme da essi prodotto ha un'influenza sugli operatori del settore.

Seppur entrambi i prodotti legislativi siano riferiti al tema della cybersicurezza, i destinatari e gli obiettivi hanno delle peculiarità differenti a seconda del sostrato normativo affrontato, ciò che preme approfondire per il prosieguo della trattazione è l'emersione di un «*mercato della cybersicurezza*» il c.d. *digital single market* che si

---

dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.»

2 In ossequio a quanto esposto sinora v. Direttiva UE 2016/1148 del Parlamento Europeo e del Consiglio, 6 luglio 2016 recante misure «*per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione Europea*»

3 Al fine di una disquisizione più lineare si consiglia la lettura costituzionale e analitica dell'Art. 41 Cost.: «Libertà dell'iniziativa economica privata. *L'iniziativa economica privata è libera. Non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana. La legge determina i programmi e i controlli opportuni perché l'attività economica pubblica e privata possa essere indirizzata e coordinata a fini sociali.*»

4 Per approfondire il tema del compromesso dialettico tra sovranità nazionale e sovranazionale in materia di *lex mercatoria* si consiglia la lettura, F.CINTIOLI, *Concorrenza, istituzioni e servizio pubblico,* Milano, 2010, EAN 9788814153891; pp. 11 ss.; cfr. Corte di Giustizia dell'Unione Europea, sentenza n. 270/2010.

5 Cfr. G. CASSANO, S. PREVITI, *Il diritto di internet nell'era digitale,* Roma, 2020, ISBN: 9788828821588; pp. 185-187.

sostanzia su certificazioni UE sulla base di più livelli, così da dare ai singoli consociati *l'aut-aut* consapevole composto da probabili rischi sull'acquisto di prodotti ICT; ciò detto rappresenta l'obiettivo – almeno quinquennale – che l'Unione Europea si prefigge in virtù di risorse al momento inadeguate come evidentemente esposto dall'ENISA.

Siffatti sistemi di certificazione sono in potenza di basarsi sui *common criteria* costitutivi degli standards ISO (*Organizzazione Internazionale per la Standardizzazione*) sulla base di una metodologia di valutazione univoca ovvero sui cc.dd. *ITSEC (Information Technology Security Evalutation Criteria)* riconosciuti, appunto, a livello comunitario.

La sopracitata fonte unionale non può esulare da una precisazione di carattere civilistico, inficiare i criteri comuni degli *standards* è, in nuce, causa del sorgere di responsabilità; nell'illecito penale la responsabilità nasce dalla commissione di un fatto criminoso cui si lega una concezione atomistica attraverso la quale ogni condotta è specificatamente prevista dalla legge, per l'illecito civile relativo al trattamento dei dati non sussiste una rigida elencazione, tutt'altro, una formula simile a una clausola, distinta per la sua vaghezza, che nasce dalla lettura in combinato disposto degli artt. 2043, 2050 e 2059 del codice civile conforme a un'interpretazione costituzionale relativa all'estrinsecarsi della persona umana quale idea-guida e valore primario del sistema ordinamentale.[6]

1.2 L'impatto dell'ENISA sui sistemi di certificazione. Postulare la c.d. *privacy by design.*

La *European Network and Information Security Agency (ENISA)* è sorta il 14 marzo del 2004, ma soltanto nel 2005 la compagine unionale la riconosce come entità legale con la ratio di rafforzare la coordinazione europea in materia di sicurezza delle informazioni, infatti, tutt'ora lo *scope* è quello di sublimare un alto livello di information and network security nella comunità assistendo la Commissione

6 G. CHIAPPETTA, Lezioni di diritto civile, Napoli, 2018, ISBN: 9788889464359, p. 8 ss. «Le situazioni inviolabili della persona umana rappresentano, quindi, una categoria aperta esplicazione della singola persona umana idea-guida e valore primario del sistema ordinamentale». Cfr. M. R. CATTANI, Il nuovo sistema diritto, Milano- Torino, 2015, ISBN: 9788861602540, pp. 300 ss.; Per quanto concerne il valore della persona umana nell'ordinamento v. P. PERLINGIERI, Trattato di diritto civile del Consiglio nazionale del notariato, Camerino, 2012, ISBN: 9788849523133, p. 11: «La preminenza del valore della persona, pertanto, si manifesta pure nella sua attitudine a porsi come principio di interpretazione e di conformazione delle norme. Difatti, l'intensità con cui l'articolo 2 Cost. tutela il valore della persona dimostra che il parametro è da annoverare tra i criteri destinati a conformare l'intero sistema normativo».

europea, gli Stati membri e di conseguenza gli operatori economici sensibilizzando e favorendo un'efficacia conoscitiva degli assunti in materia di cyber sicurezza.[7]

La previgente normativa ha avuto l'onere di costruire, da una sorta di *tabula rasa*, un sistema di fonti di regolazione del trattamento dati in grado di garantire flessibilità e specificità coinvolgendo, *de facto*, destinatari delle norme nella parte redazionale di legislazione integrativa nella quale un ruolo preponderante spettava alle autorità indipendenti; a tal fine i codici di condotta per il trattamento dei dati personali, già ai prodromi – nel 1995 – non erano una semplice manifestazione dell'autonomia negoziale privata, bensì un'innovazione della modalità di disciplina dei settori altamente tecnici e trasversali tanto da premere su una collaborazione sempre più stretta tra realtà pubblica e privata: tale sinallagma si comprende dal fatto che, benché accreditati dall'ordinamento generale, tali codici di condotta erano obbligatoriamente sottoposti all'esame dell'autorità nazionale, la quale, agendo come garante, approvava la *compliance* alle disposizioni nazionali e sovranazionali; si tratta di un passo neutrale nelle forme di autoregolamentazione libera poiché condizionate dal procedimento istruttorio dell'attività pubblica, il Garante per la protezione dei dati dà l'immagine di questo istituto tramite una definizione, ovverosia, «*autonomia assistita*».

Analogamente a quanto sopra descritto, anche i meccanismi di certificazione, marchi e sigilli presentano analisi interessanti; sono, infatti, forme di attestazione su base volontaria della compliance del trattamento dei dati effettuato dal titolare – o dai titolari solidalmente - del trattamento ovvero dal responsabile – ovvero dai sostituti del responsabile – nella disciplina europea, rilasciate con rinnovo triennale, su richiesta, non esclusivamente dalle autorità nazionali di vigilanza bensì da appositi organismi di certificazione privati accreditati in base al Regolamento CE n. 765/2008 (per l'Italia, Accredia) su parametri di indipendenza, competenza, efficace gestione delle funzioni e imparzialità.

7 Per conoscere la sinergia ovvero la leale collaborazione tra le istitutizioni citate v. E. M. BRUNNER, M. SUTER, *International CIIP Handbook 2008/2009: an inventory of 25 national and 7 international critical information infrastructure protection policies,* 2009, London, pp. 472 ss.

Com'è noto, i *considerando 77 e 98* del *Regolamento 2016/679* [8]si riferiscono alla portata degli obblighi del titolare del trattamento, al potenziale rischio su diritti e libertà degli interessati e soprattutto all'onere probatorio in caso di attivazione della giurisdizione, orbene, nella fattispecie concreta delle certificazioni, oltre a enfatizzare l'adesione al principio metodologico della *privacy by design*, di fatto, si crea un postulato che consente agli interessati di valutare rapidamente il livello di protezione dei dati personali in relazione a prodotti e servizi (e.g. ICT) sulla base del *considerando 100* [9] del succitato Regolamento.[10]

In sostanza, il Regolamento UE 2016/679 in combinato disposto al Regolamento UE 881/19 conferisce alla certificazione dei prodotti (n.d.r. anche dei servizi e dei processi) ICT il ruolo preponderante di aumentare la titolarità organica *rectius* la fiducia nei confronti dei consumatori, siano essi entità nazionali o persone fisiche, tramite la definizione di un *quadro europeo di certificazione della cybersicurezza* volto a creare meccanismi di certificazione per attestare che servizi, prodotti e processi ICT,

8 La c.d. *Privacy by design* trova legittimazione normativa nel REG. UE 2016/679, *Considerando n. 77*:« *Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati. Il comitato può inoltre pubblicare linee guida sui trattamenti che si ritiene improbabile possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e indicare quali misure possono essere sufficienti in tali casi per far fronte a tale rischio*.»; *Considerando 98: « Per i trattamenti effettuati da un'autorità pubblica, eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, o per i trattamenti effettuati nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento. Nel settore privato le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria. Il livello necessario di conoscenza specialistica dovrebbe essere determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento. Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente.»*

9 REG. UE 2016/679, *Considerando n. 100: «Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi»*

10 Il *modus cogitandi* è più lineare se letto in conformità di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo,* Milano, 2019, ISBN: 9788892112742; pp. 924 -931.

così come recita l'articolo 46, par. 2 del Regolamento UE 881/19: «*valutati nel loro ambito sono conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita*».

A titolo di esposizione lineare, senza pretese di esausitività da parte dello scrivente, si hanno, in *nuce,* alcune caratteristiche di sistema utili alla preparazione dei nuovi standards certificativi: a) la certificazione è su base volontaria fino al 2024, in seguito la Commissione su parametri SEdC (valutazione dell'efficacia e dell'utilizzo di sistemi di certificazione europea) potrà renderla obbligatoria; b) tripartizione dei livelli dei sistemi, *di base, sostanziale, elevato* correlati alla valutazione d'impatto (DPIA); c) gli organismi di valutazione della conformità rimangono sottoposti al Regolamento (CE) n. 765/2008; d) necessità di designare, per ogni Stato membro, una o più Autorità nazionali di certificazione della cybersicurezza; e) trasgressioni e violazioni alle disposizioni previste dalla stessa certificazione della cybersicurezza sono contemplate nel titolo III del Regolamento UE 881/2019 e affidate ai singoli stati membri purché *effettive, proporzionate e dissuasive.* Base critica del ragionamento poc'anzi esposto permane l'affidamento, da parte dell'UE, ad un'Agenzia senza poteri d'intervento diretto per la sicurezza cibernetica gli assi portanti del contrasto al cyber crimine.[11]

2. Il perimetro di sicurezza nazionale cibernetica. Premesse del formante legislativo.

Il d.l. 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133 recante «*disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*».

Tramite i succitati atti normativi, il formante legislativo mira a garantire un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici degli operatori pubblici e privati, delle amministrazioni pubbliche e degli enti aventi una sede nel territorio nazionale, ma soprattutto da cui dipenda l'esercizio di una funzione essenziale dello Stato *rectius* per il mantenimento di attività civili, sociali ovvero economiche, fondamentali per gli interessi dello Stato la cui interruzione o il

11 Una visione critica è riscontrabile in B. BRUNO, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali,* in *Federalismi,* n. 14/2020, ISSN: 18263534; pp. 16- 19; cfr. L. BROTHERSTON, A. BERLIN, *La sicurezza dei dati e delle reti aziendali, Defensive Security Handbook*; Milano, ISBN: 9788848136150; pp. 68 – 71.

malfunzionamento, anche non totali, potrebbero recare un pregiudizio per l'intera sicurezza nazionale.

La ratio che si sottolinea – e appare lapalissiana – non è tanto quella di estendere la portata applicativa – materiale e territoriale – del Perimetro di Sicurezza Nazionale Cibernetica ad ogni operatore del settore, bensì la sensibilizzazione verso una culture della gestione del rischio cibernetico ergo una progressiva implementazione di *incident handling* verso precisi destinatari: a) aventi sede nel territorio nazionale; b) esercenti funzioni essenziali per lo Stato; b1) all'interno di tale contenitore solo i casi specifici in cui dal malfunzionamento o interruzione, ovvero utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici possa derivare un pregiudizio per la sicurezza nazionale.[12]

La relazione tecnica del Senato sul tema sinora esposto enfatizza l'attuazione delle previsioni programmatiche del D.l. 105/2019; orbene, l'articolo 1, comma 2, lettera a) conferma la definizione di modalità e criteri procedurali per individuare le amministrazioni pubbliche, enti e operatori pubblici e privati insiti nel Perimetro di Sicurezza Nazionale Cibernetica; l'articolo 1, comma 2, lettera b) valuta la pragmaticità dei criteri con i quali i soggetti debbano rendicontare reti, sistemi informativi e servizi informatici di rispettiva pertinenza, inclusa l'architettura componentistica; tutte utilità essenziali per raggiungere le finalità introdotte dalla normativa e in relazione delle quali opereranno misure e obblighi.[13]

2.1 Fenomenologia applicativa del Perimetro di Sicurezza Nazionale Cibernetica: i D.P.C.M..

Nel dettaglio, l'applicazione concreta del D.l. 105 del 2019, al fine di depauperare discontinuità nei servizi relativi a sicurezza di reti, sistemi informativi e servizi informatici necessari, è demandata all'emanazione di D.P.C.M., da adottare su proposta del CISR (Comitato Interministeriale per la Sicurezza della Repubblica) previo parare delle competenti Commissioni parlamentari.

Primo tra questi il D.P.C.M. n. 131 del 30 luglio 2020, pubblicato in G.U. del 21 ottobre 2020, n. 261 recante il «*Regolamento in materia di perimetro di sicurezza nazionale cibernetica*» entrato poi in vigore dal 5 novembre dello stesso anno.

12 Al fine di approfondire il campo di applicazione di tale disciplina si consiglia la lettura G. CASSANO, S. PREVITI, *Il diritto di internet nell'era digitale,* Roma, 2020, ISBN: 9788828821588; pp .185-187; Cfr. S. THOBANI, *Il danno non patrimoniale da trattamento illecito dei dati personali,* in *Il diritto dell'informazione e dell'informatica,* anno XXXII, Fasc. 2- 2017, ISSN: 2499-2437, pp. 428- 430

13 Si vedano le fonti ufficiali: Senato della Repubblica Italiana, atto del Governo n. 177, Roma, giugno 2020, nota di lettura n. 154; pp. 2- 8.

Attualmente è sottoposto a parere parlamentare anche uno schema di D.P.C.M. in materia di «*regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici ex art. 1 comma due, lettera b) del D.l. 105/2019*».

La trattazione non può esimersi dall'esplicazione procedurale della sopracitata *incident handling* ad hoc – una delle finalità degli atti normativi del settore; vige un obbligo di notifica entro sei ore – quantitativamente diversificato rispetto alle ventiquattro della Direttiva NIS – presso il *Computer Security Incident Response* – Team Italia (CSRI) all'interno del Dipartimento delle Informazioni per la Sicurezza della Presidenza del Consiglio dei ministri (DIS); è obbligatorio poi notificare al Centro di Valutazione e Certificazione Nazionale (CVCN) qualora si intenda procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati ad essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici rientranti nel Perimetro di Sicurezza Nazionale Cibernetica. Se la fattispecie concreta, invece, riguarda una grave violazione sarà inevitabile il coinvolgimento e l'attivazione del Nucleo di Sicurezza Cibernetica (NSC).

Gli adempimenti contenuti nell'art. 7 del D.P.C.M. si sostanziano nella predisposizione ovvero l'aggiornamento, con cadenza specifica *rectius* annuale, dell'elenco dei beni ICT, di rispettiva pertinenza, con la nomenclatura delle reti, dei sistemi informativi e dei servizi informatici che li compongono.

Una volta ricevuta la comunicazione, i soggetti inclusi nel perimetro dovranno effettuare un'analisi di rischio (cfr. DPIA) per ogni funzione essenziale o servizio essenziale.

I soggetti facenti parte del Perimetro dovranno, dunque, individuare tutti i beni ICT necessari a svolgere la funzione o il servizio essenziale e svolgere per ognuno un'analisi dei rischi (*Risk Assessment*).[14]

Recentemente, il sistema nazionale di sicurezza cibernetica ha trovato ulteriore realizzazione nel DPCM 13 aprile 2021, n. 81 denominato «*Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lett. B), del decreto-legge 21 settembre 2019, n. 133 e di misure volte a garantire elevati livelli di sicurezza*».

Com'è noto, un incidente ai sensi del Regolamento UE 2016/679 è così enucleato: «*ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici*».[15]

14 In tal senso, in subiecta materia v. Camera dei deputati, servizio studi XVIII legislatura, *Provvedimento D.l. 105/2019: Perimetro di Sicurezza Nazionale Cibernetica*

15 DPCM 81/2021, art. 1, comma 1, lett. H

Il fine ultimo del provvedimento in oggetto, in ossequio a quanto definito dal Regolamento appena citato, è quello di neutralizzare ovvero ridurre al minimo la possibilità che questi incidenti possano sopraggiungere e quindi compromettere la c.d. *business continuity*; invero, si confà di una tassonomia precisa degli incidenti, descritti analiticamente e divisi in due categorie: a seconda dei tempi di notifica, rispettivamente di un'ora, qualora siano più gravi, e sei ore, qualora si tratti di incidenti meno gravi; confermando, de facto, la dualità del D.P.C.M. precedente[16]

3. ICT practices and career development. Il caso *e- portfolio.* Il surplus dell'uomo-macchinico.

In via preparatoria, nell'analisi dei *new media* de delle nuove *tecnologie dell'informazione e della comunicazione*, è interessante considerare il fenomeno della «*ricerca della straordinarietà*», ovverosia che tali strumenti trasformano ogni aspetto della vita quotidiana in eventi eccezionali, sicché fatti banali, una volta resi pubblici sui Social Network Sites, acquisiscono un senso di straordinarietà, il valore, dunque, non sta tanto nella conservazione della tradizione, bensì nel nuovo, nella ricerca costante di ciò che scardina riferimenti costanti e stabili; tuttavia, la sublimazione del tema porta anche benefici, primo tra tutti è la «*progressione delle carriere tramite ICT*» accentuata dall'attenzione del Governo non esclusivamente sul Perimetro di Sicurezza Nazionale Cibernetica di cui sopra, ma anche sul Ministero ad hoc dedicato all'*innovazione tecnologica e alla transizione digitale* dell'attuale Governo Draghi. [17]

La pervasività delle ICT ha profondamente rinnovato consolidati rapporti giuridici nonché linee di sviluppo sociale, basti pensare alle ingenti novelle normative in materia di protezione dei dati personali sul cyber-risk, di cui pochi comprendevano il funzionamento fino a un decennio fa; ciò che è noto, tuttavia, è l'intreccio tra potere delle tecnologie dell'informazione e potere politico: *clonabilità, immaterialità e ubiquitarietà*, mentre la persona fisica è galeotta della propria fisicità, l'*alias* virtuale può proiettarsi dovunque lui voglia.[18]

16 DPCM 81/2021, All. A

17 Un sito dedicato, voluto dal potere esecutivo, esplica le ragioni della transizione digitale v. Ministro innovazione tecnologica e transizione digitale; Sul tema della ricerca della straordinarietà, ormai lapalissiana nell'azione quotidiana di qualsivoglia consociato v. R. GHIDELLI, S. RIPAMONTI, T. TARTUFERI, *Società che cambiano,* Bologna, 2018, ISBN: 9788808720726; pp. 155 ss.

18 Una importante pronuncia giurisprudenziale che fa da scuola all'intera letteratura giuridica sul tema, partendo dal celebre caso Soraya Esfandiari è Cass., 27 maggio 1975, n. 2129, in *Giur.it.,* 1976, I, 1, 970; cfr. V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *I dati personali nel diritto europeo,* Milano, 2019, ISBN:

Alla teoria va sempre allegata una valida prassi, un caso pratico è rappresentato elegantemente dallo *European Center for the Development of Vocational Training,* che per descrivere l'esperienza italiana in materia di ICT cita il c.d. *e- portfolio,* una *repository* di esperienze, qualifiche, competenze, finalizzata a mantenere aggiornato lo *status quo* delle persone fisiche dalla prospettiva educativa, accademica e professionale; in particolare con le sezioni a) me; b) me and work; c) me and training; d) me over work; e) my skills; f) my evidence; g) documents; h) practitioner; il ruolo delle ICT nel contesto di e-portfolio è la combinazione con elementi *offline,* la connessione con le terze parti *rectius* fornitori (e.g. LMI, PES, etc…), la personalizzazione dell'information storage nonché la creazione dell'intera infrastruttura digitale dello strumento.[19]

L'intera architettura delineata nella trattazione estrinseca il rapporto tra *macchina e uomo*, un'integrazione che incide sul paradigma ontologico e assiologico dell'umanità: l'uomo diviene catalizzatore di dati passati, presenti e futuri. [20]

9788892112742; pp. 1245 – 1262.

19 CEDEFOP, *Handbook of ICT Practices for guidance and career development,* 2018, Lussemburgo, ISBN: 9789289626866; pp. 135 ss. Nel quale si fa espresso riferimento anche alle c.dd. *Tecnologie dell'Informazione e della Comunicazione* nel comparto scolastico che produce una diacronia didattica e una complicità tra docente e discente

20 E. CATERINI, *L'intelligenza artificiale «sostenibile» e il processo di socializzazione del diritto civile,* Napoli, 2020, ISBN: 9788849541601; pp. 55 ss; Cfr. P. PERLINGIERI, Manuale di diritto civile, Napoli, 2018, ISBN 978-88-495-3735-2 pp.184- 187