FOCUS

LA COMPLESSITÀ DELLA COMUNICAZIONE D'EMERGENZA E IL POSTO DEGLI ALGORITMI[1]

Enzo Cevolin

SOMMARIO: 1. Diritti digitali e comunicazione del rischio e dell'emergenza. **- 2.** Società del rischio e comunicazione. **- 3.** Comunicazione e Social media. **- 4.** Comunicazione d'emergenza e social media e algoritmi. **-** Bibliografia.

1. Diritti digitali e comunicazione del rischio e dell'emergenza.

Già nel 1979 Simon Nora e Alain Minc, nel Rapporto sull'informatica al presidente della repubblica francese nel coniare il neologismo *telematica*, formato dalla fusione tra telecomunicazioni e informatica, ne avevano intuito l'essenza rivoluzionaria che avrebbe sovvertito i tradizionali rapporti di forza che governano la società contemporanea[2] dando il via a quella che è stata definita Rivoluzione digitale e va ricompresa in una serie di rivoluzioni industriali susseguitesi nel tempo, veicolate dalle c.d. "Tecnologie Abilitanti", ovvero tecnologie con un forte impatto non solo sulla produzione ma anche sull'economia e sulla società: così la prima rivoluzione industriale con l'invenzione della macchina a vapore ha prodotto il passaggio dalla produzione manuale ad una prima meccanizzazione della produzione e alla urbanizzazione delle persone; la seconda rivoluzione industriale, con la scoperta dell'elettricità e l'uso del petrolio ha portato attraverso l'introduzione della catena di montaggio in ambito industriale alla produzione di massa; la terza rivoluzione industriale, detta anche Rivoluzione Digitale, che dagli anni sessanta, grazie all'introduzione nelle realtà produttive dell'*Information Technology* di prima generazione come microelettronica, transistor, circuiti integrati, semi-conduttori, microprocessori, *Personal Computer,* è perfezionata fino all'avvento e successiva diffusione di Internet negli anni novanta, consentendo una progressiva automazione della produzione e incidendo profondamente sui settori bancario, dell'energia e delle telecomunicazioni; infine la quarta rivoluzione industriale, che stiamo vivendo oggi, caratterizzata dall'"egemonia del dato", dall'uso estensivo in ambito industriale delle tecnologie digitali, da una stretta sinergia tra

1 *Questo documento è in adempimento del programma di ricerca presso l'Università degli Studi di Udine intitolato "Online data e comunicazione d'emergenza: metodologie e tecniche di AI per l'analisi dei contenuti digitali" SSD: M-STO/07 (responsabile scientifica, Emanuela Colombi) e del relativo assegno di ricerca attribuito al progetto "PSD_2022_2025_DMIF_Ric_Interdip." (CUP G23C22002640001).*

2 Nora S., Minc A., (1979) Convivere con il Calcolatore. Rapporto sull'informatica al presidente della repubblica francese,(1979,1984) Bompiani, Milano.

manifattura e servizi e da una progressiva riorganizzazione della società[3]. Le ultime tappe della rivoluzione digitale che riguardano in modo determinante la comunicazione sono scandite dall'evoluzione di internet in base alla tecnologia *Web*, che si riferisce ai mezzi attraverso i quali i computer comunicano tra loro utilizzando linguaggi di markup e pacchetti multimediali[4]. Dal 1990 al 2000, *Web* 1.0, con l'invenzione di Tim Berners Lee nel 1989 del *world wide web*, che permetteva la consultazione collettiva via Internet di pagine web raggiungibili tramite link: l'internet dei contenuti, contrassegnato da siti web statici, realizzati in semplice HTML, con una frequenza di aggiornamento ridotta, in cui solo i *webmaster* avevano le competenze tecniche necessarie e gli strumenti per aggiornare un sito internet e gli utenti potevano solo usufruire dei contenuti senza creare interazione, secondo la definizione del suo inventore sono stati gli anni dell'"*only read web*". Gli anni 2000-2006, Web 2.0, termine coniato ufficialmente nel 2004 da Dale Dougherty, vicepresidente di O'Reilly Media, definito anche "*read and write web*", caratterizzato dall'introduzione dei linguaggi di programmazione dinamici che hanno permesso all'utenza non tecnica di interagire con i contenuti dei siti internet: attraverso *Blogs, Wiki, Social Network, Forum* è stata possibile la partecipazione attiva degli utenti alla costruzione, classificazione e distribuzione dei contenuti. Dal 2006, Web 3.0, la cui idea di base è definire i dati della struttura e collegarli per una scoperta, automazione, integrazione e riutilizzo più efficaci tra varie applicazioni: noto anche come Web semantico tenta di collegare, integrare e analizzare dati provenienti da vari set di dati per ottenere un nuovo flusso di informazioni, in grado di esporre le cose con un approccio comprensibile al computer, in altri termini lo scopo principale del web semantico è quello di rendere il web leggibile dalle macchine e non solo dagli esseri umani. Infine ancora in fase nascente ai nostri giorni il Web 4.0, noto anche come Web simbiotico, alla base del quale vi è l'interazione tra esseri umani e macchine in simbiosi: sarà il "*read-write-execution-concurrency web*", dove le macchine sarebbero in grado di leggere i contenuti del web e di reagire sotto forma di esecuzione e decidere cosa eseguire per primo per caricare i siti web velocemente con qualità e prestazioni superiori e costruire interfacce più efficienti e controllabili, in altri termini inizierà a funzionare come un sistema operativo, complementare al cervello umano.

Durante questa rivoluzione tecnologica, inizialmente alcune società private hanno iniziato a fornire servizi volti a razionalizzare e rendere reperibili in modo semplice l'enorme mole di informazioni destrutturate presenti sulla rete Internet. Questi soggetti, i motori di ricerca prima e i social media poi, con i loro algoritmi stabiliscono la rilevanza delle informazioni e come portieri dell'informazione nel cyberspazio (c.d. *gatekeepers*) detengono le chiavi della rete, dando senso alla navigazione degli internauti nel *mare magnum* di internet diventando dei giganti dell'informazione, i c.d. *Over the Top* (OTT)[5], che "grazie ad una gerarchia liquida, al carattere globale e a-territoriale della rete, al suo travalicare ordinamenti e confini, alla rapidità con la quale le tecnologie mutano e alla volontà iniziale degli Stati di omettere una regolamentazione organica del settore al fine di favorire un nuovo mercato che era apparso sin da subito fiorente, gli OTT si sono mostrati sempre più sfuggenti ad una regolamentazione pubblicistica"[6]. Le politiche legislative dei vari paesi intervennero via via in ordine sparso a seconda delle esigenze ed emergenze: così il Regno Unito con il *Copyright,*

3 K. Schwab, La quarta rivoluzione industriale, Franco Angeli, 2016.

4 Patil H., Surwade Y., (2018). Web Technologies From Web 2.0 To Web 4.0., in IJSART, Vol. 4, April 2018, pp.810-814.

5 AGCOM definisce gli OTT «imprese prive di una propria infrastruttura e che in tal senso agiscono al di sopra delle re- ti, da cui Over-The-Top» e che «forniscono, attraverso le reti IP, servizi, contenuti e applicazioni (. . .) e traggono ricavo, in prevalenza, dalla vendita di contenuti e servizi agli utenti finali (. . .) e di spazi pubblicitari». Cfr. AGCOM, Relazione Annuale 2012 sull'attività svolta e sui programmi di lavoro, p. 28.

Designs and Patents Act del 1988, gli USA con *Digital Millennium Copyright Act* (DMCA) del 1998, l'Italia con il decreto legislativo 518 del 1992 che estendeva la disciplina sul diritto d'autore italiana (legge n. 633 del 1941) ai software.

Solo tra gli anni 2000 e 2022, l'Unione Europea ha prodotto una normativa fondata sui principi fondamentali, a cominciare dalla Carta dei diritti fondamentali dell'Unione europea che "riconosce la tutela dei dati personali come un diritto fondamentale della persona, con una sua specificità ed autonomia, e non soltanto come un aspetto, magari implicito, di una più generale tutela della vita privata. Ai dati personali, infatti, la Carta dedica l'intero articolo 8, anche con un esplicito riferimento alla necessità di una autorità indipendente di controllo, che così si configura come un ineliminabile diritto del cittadino, come un elemento costitutivo del sistema delle garanzie", delineando "un modello europeo che - attraverso convenzioni, direttive, legislazioni nazionali - è progressivamente andato oltre un´idea di *privacy* come puro scudo protettivo contro invasioni esterne" giungendo a definire "un diritto all'autodeterminazione informativa", come "potere di governare il flusso delle proprie informazioni come parte integrante di quella "costituzionalizzazione" della persona che rappresenta uno degli aspetti più significativi delle attuali dinamiche istituzionali[7]". Tale processo è colto nella sua essenza dalla Comunicazione del 26 gennaio 2022 della Commissione al Parlamento Europeo, al Consiglio al Comitato Economico e Sociale Europeo e al Comitato delle Regioni relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali che: a) mette al centro le persone; b) sostiene la solidarietà e l'inclusione, tramite la connettività, l'istruzione, la formazione e le competenze digitali, condizioni di lavoro giuste ed eque nonché l'accesso a servizi digitali online; c) ribadisce l'importanza della libertà di scelta nelle interazioni con gli algoritmi e i sistemi di intelligenza artificiale e in un ambiente digitale equo; d) promuove la partecipazione allo spazio pubblico digitale, aumenta la sicurezza e la protezione e conferisce maggiore autonomia e responsabilità nell'ambiente digitale, in particolare per i bambini e i giovani, garantendo nel contempo il rispetto della vita privata e il controllo individuale sui dati; e) promuove la sostenibilità[8]. Frutto di questo processo legislativo incentrato sulla persona e i diritti e le libertà fondamentali sono le: la direttiva copyright di recente riforma (diretti- va 2019/790/UE), la direttiva *e-Commerce* (direttiva 2000/31/CE), il GDPR (regolamento Ue 2016/679), la Framework Directive sulle reti e i servizi di comunicazione(2002/21/CE), la direttiva Audio Video Media Service (AVMS) (direttiva 2010/13/Ue), la direttiva per la protezione dei consumatori (direttiva 2011/83/UE), , il Codice di condotta sull'*hate speech*[9], l'*Artificial Intelligence Act,* Proposto dalla Commissione europea il 21 aprile 2021 e approvato dal Parlamento europeo il 13 marzo 2024, in attesa del via libera definitivo del Consiglio. Gli esiti più recenti di tale processo legislativo europeo sono il Digital Services Act – DSA (regolamento Ue 2022/2065) e il Digital Markets Act – DMA (regolamento Ue 2022/1925) con "l'idea normativa ambiziosa di disciplinare il mercato a un livello elevato di complessità

6 Montagnani E., (2021), La comunicazione pubblica on-line e la digitalizzazione delle Pubbliche amministrazioni tra pandemia e infodemia, in RID, 1-2021, pp.103-137, p.106.

7 Rodotà S., (2000), Discorso del prof. Rodotà di presentazione della "Relazione per l'anno 2000", reperibile in www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1335256

8 Comunicazione del 26 gennaio 2022 della Commissione al Parlamento Europeo, al Consiglio al Comitato Economico e Sociale Europeo e al Comitato delle Regioni relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali (COM/2022/27), online: eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52022DC0027&from=EN

9 European Commission, The EU Code of conduct on countering illegal hate speech online. Reperibile online: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

e di farlo in anticipo sugli altri legislatori mondiali, di contare cioè sul c.d. "*Brussels effect*", ossia l'effetto trainante della normativa europea, che tende a creare standard *de facto* a livello globale", in un'ottica realistica, fondata sulla constatazione che "se non possiamo competere in tecnologia, competiamo in diritto, assicurando i nostri valori, cercando di creare le condizioni perché altri li replichino"[10].

L'efficacia extraterritoriale della normativa europea non è un semplice auspicio, ma una realtà, basti pensare al caso Schrems I e II presso la corte di Giustizia dell'Unione Europea sull'applicazione del principio sancito dal Capo V del GDPR (regolamento Ue 679/2016), in base al quale ex art.44 vige un divieto di trasferimento di dati personali dal territorio dell'UE verso paesi terzi, salvo che, nei paesi di destinazione si abbia un livello di protezione del diritto alla tutela dei dati personali sostanzialmente analogo a quello del regolamento Ue. Il Regolamento prevede che tale valutazione sia effettuata direttamente dalla Commissione Ue:

a) con l'adozione di una apposita *decisione di adeguatezza* (art.45 GDPR) in esito a una approfondita analisi di molteplici fattori presenti nel paese di destinazione, tra i quali vi sono: lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale, così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati, l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo;

b) oppure, in caso di assenza di una decisione di adeguatezza approvata da parte della Commissione Ue ai sensi dell'art. 45, § 3, il titolare potrà trasferire dati in paesi terzi solo in presenza di «garanzie adeguate», «diritti azionabili» e «mezzi di ricorso effettivi» (art.46 GDPR), attraverso l'inserimento di accordi tra le parti oggettivizzati in base a *clausole tipo* (art.46, §2, lett. C) GDPR) approvate dalla anch'esse Commissione, alle quali ricorrere per cercare di garantire detto livello minimo di adeguatezza degli standard di tutela accordati ai dati personali. Ma tali accordi andranno comunque valutati dai singoli titolari alla luce dell'effettivo contesto in cui dette clausole dovranno essere applicate nei paesi di destinazione.

Nel primo caso la Commissione verifica *in concreto* con un esame complesso l'effettivo livello di sostanziale adeguatezza di tutela dei dati personali all'interno del singolo paese, mentre nel secondo caso la Commissione si limita a verificare *in astratto* che le clausole di protezione tipo possono condurre al medesimo risultato in termini di garanzie prodotte rispetto al modello europeo, ma solo tra le parti e non con riferimento al contesto di operatività delle stesse e alle specifiche caratteristiche dei singoli paesi terzi nei quali dette clausole saranno in seguito adottate: tale onere sarà di competenza quindi non della Commissione ma delle parti (punto 130 della Sentenza), rimanendo così "in capo al titolare, in collaborazione con il destinatario nel paese terzo, valutare di volta in volta se in base al contesto di operatività delle clausole, queste siano sufficienti o meno a garantire il livello di adeguatezza minimo previsto dal RGPD e dove tale standard non sia raggiunto, è onere delle parti prevedere ulteriori clausole o garanzie supplementari (così come previsto ai Considerando 109, 108 e 114 del Regolamento richiamati dalla Sentenza) funzionali a elevare il livello di tutela, o, diversamente, sospendere tale trattamento"[11]. I giudici di Lussemburgo hanno stabilito che nel caso della decisione di adeguatezza, ex art. 45, la valutazione si fondi

10 Bolognini L. et al., (A cura di), (2023), Bolognini L., Pelino E., Scialdone M., (A cura di), (2023), Digital Services Act e Digital Markets Act, Giuffrè, Milano.

11 Bellomo G., (2020), Trasferimento di dati personali verso paesi terzi: la Corte annulla il «Privacy Shield», amplia i poteri delle autorità di controllo e responsabilizza ulteriormente i data exporters, in Note e commenti - DPCE on line, 2020/4, online: https://www.dpceonline.it/index.php/dpceonline/article/view/1219 .

sulle disposizioni dello stesso GDPR lette alla luce dalla Carta dei diritti fondamentali dell'Ue, non già dei diritti garantiti negli Stati membri (punto 101 della Sentenza), né di quelli sanciti dalla CEDU (punto 98 della Sentenza). In particolare la Corte di Giustizia dell'Unione Europea ha dichiarato con la sentenza n.311 del 16 luglio 2020 non sussistere negli USA un livello di protezione sostanzialmente equivalente a quello garantito nell'Unione Europea (punto 191 della Sentenza) e conseguentemente per violazione dell'art. 45, par. 1 del GDPR, alla luce degli artt. 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea ha ritenuto non valido ai fini del trasferimento dei dati il «*Privacy Shield*» o «scudo per la *privacy*», adottato dalla Commissione con la decisione (UE) 2016/1250, che dichiarava, in caso di rispetto delle condizioni previste all'interno dello stesso, l'adeguatezza della protezione dei dati personali nel trasferimento di dati personali verso gli USA[12]. Quell'approccio alla riforma digitale dell'Unione europea sopra descritto che è stato definito antropocentrico[13] e che consiste nel voler porre al centro di ogni aspetto i valori fondanti dell'Unione europea e soprattutto il rispetto della persona, della sua dignità, la non discriminazione e la protezione dei dati[14], come si vede in questa sentenza è stato fatto proprio anche dalla Corte di Giustizia Europea, che è arrivata a censurare una decisione di adeguatezza della stessa Commissione relativa al trasferimento dei dati personali in USA.

La fondamentale importanza per l'Unione europea di questo orientamento in materia è avvalorata dal fatto che la base giuridica all'adozione di una nuova cornice normativa per i trattamenti dei dati personali, con al centro la protezione dei diritti e delle libertà fondamentali delle persone fisiche, è stata resa possibile grazie alle modifiche intercorse nel tempo ai trattati cardine del diritto europeo e, specificamente, grazie all'introduzione dell'art. 16 del TFUE, secondo paragrafo, che conferisce infatti al Parlamento europeo e al Consiglio la possibilità di stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e le norme relative alla libera circolazione di tali dati[15]. In sintonia con questo orientamento è anche la scelta dell'Unione Europea di abbandonare la via passata dell'armonizzazione attraverso direttive (95/46/CE, 2002/21/CE, 2002/58/CE), e di preferire attraverso lo strumento del regolamento l'adozione diretta delle regole sul trattamento dei dati per la realizzazione degli obiettivi, tra loro complementari, della protezione delle persone fisiche e della libera circolazione dei dati personali. Infatti il GDPR chiarisce che: «il trattamento dei dati dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri

12 Corte di giustizia dell'Unione europea, grande sezione, 16/07/2020, n.311. Sentenza nella causa C-31 1/18 Data Protection Commissioner/ Maximilian Schrems e Facebook Ireland (c.d. sentenza Schrems II), online: https://curia.europa.eu/juris/liste.jsf?nat=or&mat=or&pcs=Oor&jur=C%2CT%2CF&num=C-311%252F18&for=&jge=&dates=&language=it&pro=&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&oqp=&td=%3BALL&avg=&lg=&page=1&cid=2562948

13 Comunicazione del 26 gennaio 2022 […](COM/2022/27), cit., p.1.

14 Muto G., (2023), La digitalizzazione nell'UE: una sfida costituzionale in Media Laws – Rivista di Diritto dei Media, 21-02-2023, https://www.medialaws.eu/rivista/la-digitalizzazione-nellue-una-sfida-costituzionale/

15 Gambino A. M., Mula D., Stazi A., (2021), Diritto dell'informatica e della comunicazione, Giappichelli, Torino, p.80; Cfr. TFUE Articolo 16, Co.2: "Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti" e art. 1, comma 2, Reg 679/2016 UE: "Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali".

diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica» (considerando 4 del regolamento Ue 679/2016). Coerentemente il GDPR è disseminato di norme che sono espressione di questa impostazione, come ad esempio quando stabilisce la liceità del trattamento dei dati indipendentemente dal consenso dell'interessato, qualora il trattamento sia necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. E il regolamento europeo specifica che in questo caso il bilanciamento fra il legittimo interesse del titolare o del terzo e i diritti e libertà dell'interessato non spetta al Garante Privacy, ma è compito dello stesso titolare e ciò costituisce una delle principali espressioni del principio di "*accountability*" introdotto dal nuovo pacchetto protezione dati[16]. Tale principio di *accountability* è a sua volta espressione dell'orientamento sopra descritto dell'Unione europea. Infatti l'art. 24, co. 1 del GDPR arriva ad anticipare la tutela fino ai soli "rischi, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche", imponendo nei confronti del titolare del trattamento di mettere in atto tutte le misure tecniche e organizzative adeguate a garantire che il trattamento sia stato effettuato conformemente alla normativa di settore, specificando la necessità di tenere in considerazione la natura, l'ambito di applicazione, il contesto e le finalità del trattamento (art. 24, n. 1), e richiedendo che tali valutazioni si concretizzino sia nella scelta delle misure tecniche e organizzative da adottare nel contesto aziendale sia nell'attuazione di *privacy policy* conformi (art, 24, n. 2). E l'art. 25 del GDPR ulteriormente specifica la necessità di configurare il trattamento dei dati prevedendo *fin dall'inizio* tutte le garanzie indispensabili alla tutela degli interessati, efficacemente sintetizzato dall'espressione inglese *data protection by default and by design*: "la tutela, pertanto, è anticipata ad un momento anteriore al trattamento dei dati personali e prevede un impegno attivo dei titolari fin dalla progettazione dei prodotti e servizi il cui utilizzo incida sui dati degli utenti"[17]. Inoltre, qualora l'uso di nuove tecnologie possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il GDPR richiede la c.d. *Data Protection Impact Assessment* (DPIA), disciplinata dagli artt.35 e 36 del regolamento, che si sostanzia in un procedimento di valutazione preventiva d'impatto sulla protezione dei dati, collocata sia "in una fase preliminare dello sviluppo del prodotto o del servizio, ovvero quando il design di quest'ultimo non è delineato in maniera definitiva", sia prima dell'attivazione del servizio, ed infine deve anche "essere ripetuta con cadenza periodica, al fine di verificare l'attualità delle misure di sicurezza"[18]. E l'art.35 GDPR impone che, tra le varie ipotesi, la DPIA sia svolta in particolare nel caso di "valutazione sistematica e globale di aspetti personali relativi a persone fisiche, *basata su un trattamento automatizzato*, *compresa la profilazione*, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche" (art. 35, §3, lett. a), regolamento Ue 679/2016).

16 Gambino A. M., Mula D., Stazi A., (2021), op. cit., p.85
17 Stanzione M. G., (2016), Il regolamento europeo sulla privacy: origini e ambito di applicazione, in Europa e Diritto Privato, fasc.4, 2016, p. 1255.
18 Gambino A. M., Mula D., Stazi A., (2021), op. cit., p.91.

Entro questo scenario europeo di governance della rivoluzione digitale, il GDPR stabilisce le norme "relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati" (art. 1, §1, GDPR), e le finalità del regolamento, che consistono nel proteggere "i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali" (art. 1, §2, GDPR), nonché l'ambito di applicazione materiale che riguarda il "trattamento interamente o parzialmente automatizzato di dati personali" e il "trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi" (art. 2, §1, GDPR). Il fulcro della disciplina del GDPR è costituito dai principi fondamentali applicabili al trattamento dei dati personali sanciti dall'art. 5 del GDPR che sono:

- i principi di liceità, correttezza e trasparenza (art. 5, §1, lettera a), GDPR). La trasparenza è un aspetto che da tempo consolidato nel diritto dell'Unione europea[19] con lo scopo di infondere fiducia nei processi che riguardano i cittadini, permettendo loro di comprenderli e, se necessario, di opporvisi. E consiste in un obbligo trasversale che si esplica in tre elementi centrali: 1) la fornitura agli interessati d'informazioni relative al trattamento corretto; 2) le modalità con le quali il titolare del trattamento comunica con gli interessati riguardo ai diritti di cui godono ai sensi del regolamento; 3) le modalità con le quali il titolare del trattamento agevola agli interessati l'esercizio dei diritti di cui godono[20]. Inoltre ai sensi dell'articolo 12, paragrafo 1 del GDPR, il titolare del trattamento deve fornire agli interessati informazioni concise, trasparenti, intelligibili e facilmente accessibili sul trattamento dei loro dati personali, precisando che per i dati raccolti direttamente dall'interessato, tali informazioni devono essere fornite al momento della raccolta (articolo 13, GDPR), mentre per i dati ottenuti indirettamente, le informazioni devono essere fornite entro i termini stabiliti all'articolo 14, paragrafo 3 GDPR. La trasparenza è infine intrinsecamente legata al nuovo principio di accountability ex art. 24 GDPR sopra citato e al principio di correttezza in relazione al trattamento dei dati personali affermato all'articolo 8 della Carta dei diritti fondamentali dell'Unione europea. Mentre la liceità fa riferimento alle basi giuridiche del trattamento ex art.6 del GDPR che sarà trattato a breve;
- il principio di limitazione delle finalità di trattamento secondo il quale i dati possono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali (art. 5, §1, lettera b), GDPR);
- il principio di minimizzazione secondo cui i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (art. 5, §1, lettera c), GDPR)
- il principio di esattezza per cui i datai devono essere veritieri, esatti e, se necessario, aggiornati e per il quale devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (art. 5, §1, lettera d), GDPR);

19 L'articolo 1 del TUE si riferisce a decisioni prese "nel modo più trasparente possibile e il più vicino possibile ai cittadini", l'articolo 11, paragrafo 2, del medesimo trattato recita: "Le istituzioni mantengono un dialogo aperto, trasparente e regolare con le associazioni rappresentative e la società civile" e l'articolo 15 del TFUE fa riferimento, fra l'altro, al diritto dei cittadini dell'Unione di accedere ai documenti delle istituzioni, organi e organismi dell'Unione e all'obbligo che incombe a questi di assicurare la trasparenza dei lavori svolti.

20 Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), online: https://ec.europa.eu/newsroom/article29/items/622227

- il principio di limitazione della conservazione per cui i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (art. 5, §1, lettera e), GDPR);
- il principio di integrità e riservatezza per cui i dati devono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali art. 5, §1, lettera f), GDPR).

L'art. 5 infine non solo obbliga il titolare del trattamento a rispetto di dei principi sopra citati, ma gli impone anche di essere in grado di provare di essersi adeguato ad essi, definendo tale ulteriore obbligo "responsabilizzazione" (art. 5, §2 GDPR), in inglese *accountability*, che sarà ripreso e meglio definito dall'art. 24 GDPR, sopra già descritto.

Per quanto riguarda le condizioni di liceità del trattamento la norma fondamentale è l'art.6 del GDPR[21] che stabilisce in via generale come base giuridica al trattamento dei dati il consenso dell'interessato (art. 6, § 1, lett. a), GDPR) che deve essere:

- in tutti i casi, libero, specifico, informato, inequivocabile e non è ammesso il consenso tacito o presunto; manifestato attraverso "dichiarazione o azione positiva inequivocabile" (art.4, n.11 GPDR);
- non necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è una modalità idonea a comprovare inequivocabilmente il consenso e il suo essere "esplicito" (per i "dati sensibili"). Inoltre, il titolare deve essere in grado di dimostrare che l'interessato abbia prestato il consenso a uno specifico trattamento (art. 7, § 1, GDPR) e se riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro, e non è vincolante qualora sia in violazione del regolamento (art. 7, § 2, GDPR). Oltre a ciò l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento (art. 7, § 3, GDPR);
- Con riferimento ai minori il consenso è valido in Europa a partire dai 16 anni (art. 8, § 1, GDPR), mentre in Italia a partire dai 14 anni (in conformità il d.lgs. n. 101/2018 che ha utilizzato l'intervallo di valori tra 16 e 13 anni concesso agli stati membri dalla normativa europea) e prima di tali soglie di età occorre raccogliere il consenso dei genitori o di chi ne fa le veci. Infine per quanto riguarda le categorie particolari di dati personali (art. 9, GDPR), i cosiddetti "dati sensibili", come accennato sopra, il consenso deve essere "esplicito", così come per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione (art. 22, GDPR).

Un'altra base giuridica al trattamento dei dati si ha in osservanza di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (art. 6, § 1, lett. b), GDPR). Ai fini della liceità di trattamento dei dati un'ulteriore condizione è l'esecuzione di un obbligo legale al quale è soggetto il titolare del trattamento

21 Così come interpretato in base alle Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679 adottate dal Gruppo di lavoro Articolo 29 (WP259 rev.01) del Comitato europeo per la protezione dei dati, Reperibile online: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_it.pdf

(art. 6, § 1, lett. c), GDPR): categoria che rinvia all'esistenza di una normativa europea o nazionale di dettaglio (art. 6, § 3, GDPR).

Una quarta base giuridica al trattamento dei dati si ha quando sia necessaria per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (art. 6, § 1, lett. d), GDPR): stando al considerando n. 46 del GDPR, si tratta di un'ipotesi residuale che si può invocare solo nel caso in cui nessuna delle altre condizioni di liceità trovi applicazione[22].

Una quinta condizione di liceità al trattamento dei dati consiste nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, § 1, lett. e), GDPR): "L'articolo si presenta come una riformulazione dell'articolo 19 del previgente codice in materia di protezione dei dati personali, il cui ambito di applicazione soggettivo viene esteso al fine di adeguarsi all'impostazione adottata dal regolamento. Nel regolamento, infatti, scompare la distinzione basata sulla natura pubblica o privata dei soggetti che trattano i dati, rilevando unicamente la finalità del trattamento perseguita, vale a dire se la finalità concerne un interesse pubblico o privato. L'articolo quindi deve intendersi applicabile ai soggetti che trattano i dati personali per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a prescindere dalla loro natura soggettiva"[23].

Infine l'ultima base giuridica al trattamento dei dati si ha in presenza di un in trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore (art. 6, § 1, lett. f), GDPR).

Un'ulteriore espressione del principio di trasparenza è l'informativa che deve essere comunicata all'interessato dal titolare del trattamento che ai sensi dell'art. 12 del GDPR "adotta misure appropriate per fornire tutte le *informazioni* di cui agli articoli 13 e 14 e le *comunicazioni* di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato". Se i dati sono raccolti direttamente presso l'interessato l'informativa deve essere comunicata prima della raccolta (Art.13, §1, GDPR) mentre nel caso in cui i dati non vengano raccolti presso l'interessato l'informativa deve essere comunicata ai sensi dell'art. 13, paragrafo 3 del GDPR: "a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati; b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali". Sia nel caso che i dati siano raccolti presso l'interessato, come in quello che non lo siano, il titolare del trattamento deve comunicare "l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali

22 Considerando n. 46 del GDPR: "Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica"

23 Relazione illustrativa del d.lgs. 101/2018 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, disponibile online sul sito della Camera dei deputati: https://www.camera.it/leg18/682?atto=022&tipoAtto=Atto&idLegislatura=18&tab=2

casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato" (art. 13, §2, lett.f) e art. 14, §2, lett. g) GDPR).

Per comprendere la presenza di un processo decisionale automatizzato, compresa la profilazione occorre guardare innanzitutto all'art. 4 del GDPR che definisce la profilazione come: "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica". Le linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679[24] indicano tre elementi perché si possa parlare di profilazione: 1) deve essere una forma di trattamento automatizzato; 2) deve essere effettuata su dati personali; 3) il suo obiettivo deve essere quello di valutare aspetti personali relativi a una persona fisica." Successivamente Le stessa linee guida chiariscono che la profilazione di cui all'articolo 4, n. 4 del GDPR fa riferimento a "qualsiasi forma di trattamento automatizzato", mentre l'articolo 22 del GDPR riguarda il trattamento "unicamente" automatizzato, che si sostanzia "nella capacità di prendere decisioni impiegando mezzi tecnologici senza coinvolgimento umano". Sempre secondo le linee guida tali decisioni automatizzate possono essere basate su qualsiasi tipo di dati forniti dall'interessato sia direttamente che indirettamente e possono essere prese ricorrendo o meno alla profilazione, la quale a sua volta può essere elaborata senza che vengano prese decisioni automatizzate, tuttavia, la profilazione e il processo decisionale automatizzato non sono necessariamente attività separate. Per meglio chiarire la differenza profilazione e processo decisionale esclusivamente automatizzato linee guida spiegano che:

- nel caso della profilazione *un essere umano decide* se sulla base di un profilo prodotto con mezzi unicamente automatizzati;
- nel caso di decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produce effetti giuridici o incide in modo analogo significativamente sull'interessato, *un algoritmo decide* e la decisione viene trasmessa automaticamente alla persona, *senza alcuna previa valutazione significativa da parte di un essere umano*.

In quest'ultimo caso l'art. 22 del GDPR stabilisce innanzitutto il diritto dell'interessato "di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona", tranne che per tre eccezioni: "a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato". Inoltre ai sensi dell'art. 9, par. 1 del GDPR un processo decisionale automatizzato che "riveli l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale", o che tratti "dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona" è permesso solo con il consenso esplicito dell'interessato o per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri. Sempre con riferimento alle decisioni basate unicamente su un trattamento automatizzato il GDPR

24 Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 adottate il 3 ottobre 2017, Versione emendata e adottata in data 6 febbraio 2018, (WP 251 rev.01): https://ec.europa.eu/newsroom/article29/items/612053

introduce l'obbligo ex l'art. 15, par. 1, lett. h), di far conoscere all'interessato l'esistenza di tale processo, e il diritto ex art. 13, par. 2, lett. f) di ottenere informazioni significative sulla logica utilizzata e nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. In considerazione dei rischi che i diritti e le libertà dell'interessato possono subire a seguito di tali trattamenti, il GDPR "da un lato obbliga il titolare del trattamento ad attuare misure appropriate "rafforzate" di tutela come prevedere con regolarità modalità a verifica della correttezza dei processi per limitare errori di classificazione o valutazione con impatto negativo sui soggetti profilati, e dall'altro lato, ex art, 22, par. 3), conferisce all'interessato il potere di ottenere l'intervento umano da parte del titolare, di esprimere la propria opinione e di contestare la decisione, nei casi in cui tale decisione sia prevista per contratto o consentita dall'interessato[25]. Un'illustre dottrina osserva: "come il GDPR abbia introdotto disposizioni atte a garantire che la profilazione e il processo decisionale automatizzato relativo alle persone fisiche (comprensivo o meno di profilazione) non siano utilizzati in maniera tale da avere un impatto ingiustificato sui diritti delle persone. Il GDPR, infatti, non si concentra soltanto sulle decisioni prese a seguito di un trattamento automatizzato o della profilazione, ma trova applicazione anche alla fase della raccolta di dati per la creazione di profili e all'applicazione di tali profili alle persone fisiche.

La profilazione dei dati personali si intreccia, evidentemente, con la tematica dei Big Data, rispetto alla quale emergono criticità legate alla privacy e alla protezione dei dati personali, in ragione della enorme mole di dati che vengono analizzati per svolgere l'attività di valutazione e previsione comportamentale che, in qualche modo, supera la semplice nozione di profilazione. Da qui l'esigenza di declinare con specifico riferimento a questo scenario non solo i principi generali in materia di protezione dei dati di cui al GDPR, ma, vieppiù, le indicazioni contenute nella Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, c.d. Convenzione 108, del 1981 e rivista nel maggio 2018, che rappresenta l'unico trattato internazionale giuridicamente vincolante di portata mondiale nel settore del trattamento dei dati" e " parallelamente, rilevano le Linee Guida elaborate dal WP29 relative alla trasparenza e ai processi decisionali automatizzati relativi alle persone fisiche e alla profilazione. Il punto cruciale per la tutela degli interessati diviene infatti, il momento informativo sulle modalità di utilizzo dei dati acquisiti, nel quale deve essere chiaramente esplicitato se tali dati saranno o meno impiegati per elaborazioni con tecniche legate ai *Big Data* e, in tal caso, illustrare, per quanto possibile, le finalità di tale trattamento. Per quanto possibile, ovviamente, in quanto i dati che compongono un'infrastruttura *Big Data* possono essere elaborati per una vasta gamma di finalità, più ampia, spesso, di quella inizialmente immaginata al momento dell'inizio della raccolta.

L'*output* informativo raramente viene, infatti, desunto dà dati che si riferiscono espressamente ad un input correlato, ma viene piuttosto desunto da correlazioni con altri dati, anche con dati di cui al momento della raccolta non si disponeva. Da qui anche la difficoltà di distinguere nettamente se il dato elaborato sia o meno personale"[26]. Si tenga presente che l'omessa o errata informativa della privacy ai sensi dell'art. 83, §5, lett. b) del GDPR è "soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente". Pertanto per la disciplina europea è obbligatorio per tutti i siti *web, social* media inclusi, inserire all'interno della propria *privacy policy*, in modo chiaro ed esaustivo, informazioni inerenti alla tipologia dei dati raccolti, alle finalità e alle modalità di trattamento dei dati, comprese

25 Morelli C., (2024), Intelligenza Artificiale, Maggioli Editore, Sanarcangelo di Romagna, 2024, p.81.
26 Gambino A. M., Mula D., Stazi A., (2021), op. cit., pp. 108-109.

informazioni in merito alla loro destinazione e al luogo in cui sono conservati o trasferiti, e al periodo di conservazione degli stessi. Dovrà inoltre essere chiara ed espressa non solo la base giuridica del trattamento, ma anche tutti i diritti esercitabili dagli utenti, i dati identificativi del titolare d trattamento e del responsabile della protezione dei dati, nonché inserire dati del sito o dell'app e del titolare del sito web e specificare l'eventuale presenza di processi decisionali automatizzati[27].

Infine, per quest'ultima eventualità va ribadita l'importanza dell'art, 22, par. 3) del GDPR che conferisce all'interessato il potere di ottenere l'intervento umano da parte del titolare, norma che va letta alla luce della Dichiarazione sui diritti e i principi digitali per il decennio digitale (2020-2030)[28], nella quale Il Parlamento Europeo, Il Consiglio e La Commissione Europea dichiarano all'art. 1 che "Le persone sono al centro della trasformazione digitale nell'Unione europea. La tecnologia dovrebbe essere al servizio e andare a beneficio di tutte le persone che vivono nell'UE, mettendole nelle condizioni di perseguire le loro aspirazioni, in tutta sicurezza e nel pieno rispetto dei loro diritti fondamentali". Tale impegno si è espresso anche nel recentissimo *Artificial Intelligence Act*, la prima legge al mondo sull'Intelligenza Artificiale - come ha dichiarato il relatore del testo Brando Benifei - che fa salva richiama la normativa del GDPR e che con un approccio basato su quattro livelli di rischio per i sistemi di IA, da minimo, a limitato ed elevato, fino a inaccettabile, prevede per il livello alto, proprio lo stesso diritto sancito dall'art. 22 del GDPR, il principio cd *human in the loop*, che impone a tali sistemi di "essere progettati e sviluppati in modo da poter essere efficacemente supervisionati da persona fisiche durante il loro uso" e permettere agli utenti/operatori di "valutare l'impatto sui diritti fondamentali prima di metterli in esecuzione e, se non possono essere individuati piani dettagliati per attenuare i rischi identificati, devono astenersi dal farlo"[29].

Come ha chiarito uno studio sulla comunicazione pubblica *on-line* che "pur essendo rintracciabile un fondamento normativo all'utilizzo dei social media da parte delle Pubbliche amministrazioni[30], tale pratica non costituisce un obbligo per la Pubblica amministrazione né un diritto del cittadino al mezzo. Vero diritto del cittadino è invece, quello di ricevere una informazione e una comunicazione pubblica di qualità al quale fa eco un dovere della

27 Imperatrice I., (2023), Tutela dei dati personali sui Social, in Martorana M., (a cura di), (2023), Diritto e Social Network, Lex Iuris, Bologna, 2023, pp.45-74, p.65.

28 European Declaration on Digital Rights and Principles for the Digital Decade: https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

29 Morelli C., (2024), op.cit., p.47.

30 Prima tra tutte la l. 150/2000. In particolare, l'art. 1 c. 4 lett. b) dispone che la comunicazione esterna rivolta ai cittadini, alle collettività e ad al- tri enti avvenga attraverso ogni modalità tecnica ed organizzativa. Altresì l'art. 2 c. 242 secondo il quale le attività di comunicazione ed informazione della PA «possono essere svolte con ogni mezzo di trasmissione idoneo ad assicurare la trasmissione dei messaggi». Ad essa si affiancano una serie di altre norme, che seppur non direttamente vanno a toccare in modo tangenziale anche i social media. Nelle Linee Guida per i siti web della P.A., in particolare all'art. 6 c. 3 relativo alla partecipazione, si afferma che «i social media possono essere considerati dalla pubblica amministrazione come canali di broadcasting ad alto potenziale di audience, dalla forma semplice e di versatile diffusione tra i cittadini, estremamente economici (sia per gli utenti che Amministrazioni pubbliche stesse), multipiattaforma e spesso interoperabili tra loro». I d.lgs. n. 179/2016 e n. 217/2017 che hanno operato una profonda rivisitazione del Codice dell'amministrazione digitale. La Circolare n. 2/2017 di "Attuazione delle norme sull'accesso civico generalizzato" nella quale si fa un uso esplicito del termine social media quale strumento utile alla "valorizzazione del dialogo con le comunità di utenti dei social media" (art. 8.2)44 , prevedendo anche che le amministrazioni pubbliche dialoghino con i giornalisti e i media che svolgono attività di social watchdog (art. 8.1) che di fatto le- gittima la pratica di utilizzare il web sociale come fonte giornalistica. Pur costituendo una libera scelta della Pubblica amministrazione, l'utilizzo dei social media pare incentivato e trovare fondamento normativo anche in tutta una serie di norme del Codice dell'amministrazione digitale decreto legislativo 7 marzo 2005, n. 82 (c.d. CAD).

Pubblica amministrazione di rimettere al centro del suo agire il cittadino e i suoi diritti di essere informato e partecipe della vita civica, anche e non solo attraverso i social media, divenuti ormai l'agorà principale nella quale i cittadini sono presenti ed abitano"[31]. Comunque qualora le amministrazioni scelgano di partecipare alla comunicazione attraverso i social "significa non solo sfruttare tecnicamente al meglio le *affordance* delle piattaforme digitali, ma gestire queste piattaforme secondo un approccio responsabile e strategico, oltre che curare tali canali in modo continuativo e *citizen oriented*"[32], ma soprattutto rispettare e adeguarsi ai principi e alla normativa sopra descritta. Ciò in modo particolare nell'ipotesi alla base del progetto di cui fa parte il presente articolo di utilizzare le moderne tecniche di AI (*Deep e Machine Learning*) al fine di valorizzare i contenuti multimediali prodotti da normali cittadini e condivisi pubblicamente online sulle piattaforme social per supportare le operazioni di gestione dell'emergenza nella comunicazione d'emergenza, dato che tale comunicazione incide su beni fondamentali delle presone.

Infine per quanto riguarda la comunicazione d'emergenza e del rischio bisogna tenere presenti gli esiti della sociologia del rischio (v. infra) che hanno indissolubilmente legato l'entità del rischio alla sua comunicazione e sono stati progressivamente assorbiti nella legislazione europea e italiana, anche se in modo più empirico, tenendo presente non tanto la dottrina sociologica, quanto il susseguirsi di eventi dannosi ed emergenze mal gestite. Infatti la prima normativa che attribuisce importanza alla comunicazione del rischio è la Direttiva 1982/501/ CEE[33], recepita in Italia con il D.P.R. 17 maggio 1988, n. 175 e denominata «Direttiva Seveso», con chiaro riferimento alla mala gestione del grave incidente industriale avvenuto il 10 luglio 1976 nell'azienda ICMESA di Meda, causa della fuoriuscita e della dispersione nell'atmosfera di una nube di diossina, una sostanza fra le più tossiche, che investì una vasta area di terreni dei comuni limitrofi della bassa Brianza e particolarmente quello di Seveso. Proprio l'art. 8, comma 1 della sopracitata direttiva stabilisce per la prima volta in capo agli Stati un obbligo di informazione in caso di incidente nei confronti della popolazione coinvolta: "Gli Stati membri vigilano affinché le persone che possono essere colpite da un incidente rilevante […] siano opportunamente informate sulle misure di sicurezza e sulle norme da seguire in caso di incidente".

Con la Direttiva 89/618/Euratom del Consiglio, del 27 novembre 1989[34] riguardante il caso dell'emergenza radioattiva, questo diritto di informazione, da indicazione generica viene definito sempre più nel dettaglio nei contenuti, nei modi e nei tempi. Ad esempio l'art. 5 specifica che la popolazione coinvolta "sia informata *sulle misure di protezione sanitaria* ad essa applicabili, nonché *sul comportamento che deve adottare* in caso di emergenza radioattiva" e che le informazioni "devono comprendere almeno gli elementi di cui all'allegato I", ovvero: "1. Nozioni fondamentali sulla radioattività e sui suoi effetti sull'essere umano e sull'ambiente; 2. Vari casi di emergenza radioattiva presi in considerazione e relative conseguenze per la popolazione e l'ambiente; 3. Misure urgenti previste per avvertire, proteggere e soccorrere la popolazione in caso di emergenza radioattiva. 4. Adeguate informazioni in merito al comportamento che la popolazione dovrebbe adottare in caso di emergenza radioattiva". Inoltre sempre l'art.5 sancisce che la popolazione sia informata "senza che essa ne debba fare richiesta" e che tali informazioni restino in permanenza accessibili al pubblico. Mentre l'art. 6 stabilisce nell'eventualità di una emergenza radioattiva

31 Montagnani E., (2021), op.cit., p.113.

32 Lovari A., (2019), Social media e pubblica amministrazione tra diritti e doveri: una prospettiva sociologica, in Rivista italiana di informatica e diritto, ISSN 2704-7318 Fascicolo 1-2019 DOI: 10.32091/RIID0006, p. 89.

33 Direttiva 1982/501/ CEE: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A31982L0501

34 Direttiva 89/618/Euratom del Consiglio, del 27 novembre 1989: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A31989L0618

che la popolazione effettivamente interessata "sia *immediatamente* informata *sui fatti* relativi all'emergenza, *sul comportamento* da adottare e *sui provvedimenti* di protezione sanitaria". Ed infine l'art. 7 differenzia l'informazione in base ai diversi pubblici preoccupandosi che i soggetti non facenti parte del personale degli impianti e/o non partecipanti alle attività definite come trasporto e stoccaggio di combustibili nucleari o di residui radioattivi, "che però potrebbero intervenire nell'organizzazione dei soccorsi in caso di emergenza radioattiva, ricevano *un'informazione adeguata e regolarmene aggiornata* sui *rischi* che l'intervento comporterebbe per la loro salute *e sulle precauzioni* da prendere in un caso simile".

Successivamente si comincia a considerare anche il *diritto dei cittadini a partecipare ai processi di pianificazione territoriale* degli impianti industriali e di valutazione del rischio, con una nuova direttiva, denominata «Seveso 2» (Direttiva 1996/82/CE)[35] recepita in Italia con il d.lgs. n.334 agosto 1999, che prevede la previa consultazione della popolazione, d'intesa con le regioni e gli enti locali interessati, per predisporre il piano dì emergenza (Art.20).

Ed ancora, dopo il grave incidente del 21 settembre 2001 agli impianti della AZF d di Tolosa, in Francia (dove una nube tossica provocò la morte di 29 persone e il ferimento di altre duemila, anche per una gestione dell'emergenza inadeguata), con l'emanazione della «Seveso 3" (Direttiva 2012/18/UE)[36], recepita in Italia con d.lgs. n. 105 giugno 2015, viene ribadita la necessità di fornire ai cittadini tempestive informazioni sui rischi, "in modo attivo, senza che il pubblico debba farne richiesta", messe a disposizione "anche in modo permanente" e "adeguatamente aggiornate" e – per la prima volta si specifica – "per via elettronica". Sempre per la prima volta la sopracitata direttiva si preoccupa di precisare che tali informazioni siano formulate "in modo chiaro e comprensibile" al pubblico, aggiungendo anche la possibilità di azioni legali richiamando eventualmente l'applicazione della Convenzione di Arhus del 1998[37] sull'accesso alle informazioni, la partecipazione pubblica ai processi decisionali e il ricorso alla giustizia nelle questioni ambientali.

In ultimo il cd Codice della Protezione Civile d.lgs. 1/2018[38] nell'indicare che le attività della Protezione civile sono quelle volte alla previsione e alla prevenzione dei rischi, al soccorso delle popolazioni sinistrate e ad ogni altra attività necessaria e indifferibile, diretta al contrasto e al superamento dell'emergenza e alla mitigazione del rischio, inserisce tra le attività di prevenzione: l'allertamento e la diffusione della conoscenza e della cultura della protezione civile, anche con il coinvolgimento delle istituzioni scolastiche, e inoltre l'informazione alla popolazione sugli scenari di rischio e le relative norme di comportamento nonché sulla pianificazione di protezione civile "allo scopo di promuovere la resilienza delle comunità e l'adozione di comportamenti consapevoli e misure di autoprotezione da parte dei cittadini".

Per concludere quando si parla di comunicazione istituzionale è necessario fare riferimento alla legge n.150/2000[39] che disciplina le attività di informazione e di comunicazione delle pubbliche amministrazioni. Gli unici riferimenti di interesse sono:

35 Direttiva 1996/82/CE: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A31996L0082

36 Direttiva 2012/18/UE: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32012L0018&from=IT

37 Convenzione sull'accesso alle informazioni, la partecipazione del Pubblico ai processi decisionali e l'accesso alla giustizia in Materia ambientale:
https://www.isprambiente.gov.it/it/garante_aia_ilva/normativa/Normativa-sull-accesso-alle-informazioni/normativa-sovranazionale/convenzione_aarhus_25_06_1998.pdf

38 Codice della Protezione Civile d.lgs. 1/201: https://www.protezionecivile.gov.it/it/normativa/decreto-legislativo-n-1-del-2-gennaio-2018--codice-della-protezione-civile/

39 Legge n.150/2000: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2000-06-07;150

- l'art.1, comma 4., che fatto salvo il rispetto delle norme vigenti in tema di segreto di Stato, di segreto d'ufficio, di tutela della riservatezza dei dati personali e in conformità ai comportamenti richiesti dalle carte deontologiche, sono considerate attività di informazione e di comunicazione istituzionale quelle poste in essere in Italia o all'estero dalle pubbliche amministrazioni e volte a conseguire: a) l'informazione ai mezzi di comunicazione di massa, attraverso stampa, audiovisivi e strumenti telematici; b) la comunicazione esterna rivolta ai cittadini, alle collettività e ad altri enti attraverso ogni modalità tecnica ed organizzativa; c) la comunicazione interna realizzata nell'ambito di ciascun ente.

- l'art.2 comma 2, che precisa che "le attività di informazione e di comunicazione sono attuate *con ogni mezzo di trasmissione idoneo* ad assicurare la necessaria diffusione di messaggi, anche attraverso la strumentazione grafico-editoriale, *le strutture informatiche*, le funzioni di sportello, le reti civiche, *le iniziative di comunicazione integrata* e *i sistemi telematici multimediali*."

Infine nella normativa l'unico riferimento specifico ai *social media* si trovava in un atto amministrativo denominato "Linee guida per i siti web della PA " previste dell'art. 4 della Direttiva n. 8/2009 del Ministro per la pubblica amministrazione e l'innovazione[40], peraltro ora abrogate dalle nuove "Linee guida di design per i siti internet e i servizi digitali della Pubblica Amministrazione ai sensi dell'art. 53, comma 1-*ter* del D. Lgs. 7 marzo 2005, n. 82, come da Determinazione 26 luglio 2022, n. 224 dell'Agenzia per l'Italia Digitale (AGID)[41] che annullano e sostituiscono le precedenti "Linee guida per i siti *web* delle PA" previste dall'art. 4 della Direttiva del Ministro per la Pubblica Amministrazione e l'innovazione 26 novembre 2009, n. 8. Comunque queste ultime alla sezione "Partecipazione e web 2.0", prima richiamavano l'applicazione:

- del Codice dell'Amministrazione Digitale (D.lgs. 7 marzo 2005, n. 82)[42] che sancendo il diritto all'uso delle tecnologie nelle comunicazioni con le amministrazioni e quello alla partecipazione del cittadino al procedimento amministrativo, riconosce di fatto l'importanza del coinvolgimento dei cittadini nella vita politica e amministrativa;
- del Decreto legislativo 27 ottobre 2009, n. 150[43], riguardo alle fasi del ciclo di gestione della performance, uno degli ambiti d'intervento del sistema di misurazione e valutazione della performance organizzativa ha per oggetto proprio il miglioramento qualitativo e quantitativo delle relazioni con i cittadini, i soggetti interessati, gli utenti e destinatari dei servizi erogati dalla pubblica amministrazione, da realizzare attraverso lo sviluppo di forme di partecipazione e collaborazione (art. 8, lettera e).

E poi continuavano proponendo l'utilizzo dei social media nei seguenti termini: "*I social media* possono essere considerati dalla pubblica amministrazione come canali di *broadcasting* ad alto potenziale di audience, dalla forma semplice e di versatile diffusione tra i cittadini, estremamente economici (sia per gli utenti che Amministrazioni pubbliche stesse), multipiattaforma e spesso interoperabili tra loro.

40 Linee guida per i siti web della PA ex art. 4 della Direttiva n. 8/2009 del Ministro per la pubblica amministrazione e l'innovazione : https://www.assemblea.emr.it/footer/documentazione/linee%20guida%20siti%20web%20delle%20pa%202011.pdf

41 Linee guida di design per i siti internet e i servizi digitali della Pubblica Amministrazione ai sensi dell'art. 53, comma 1-ter del D. Lgs. 7 marzo 2005, n. 82 : https://docs.italia.it/italia/design/lg-design-servizi-web/it/versione-corrente/index.html

42 Codice dell'Amministrazione digitale (CAD), D.lgs. 7 marzo 2005, n. 82: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82

43 Decreto legislativo 27 ottobre 2009, n. 150: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2009-10-27;150!vig=2024-03-21

Attraverso la pubblicazione in tempo reale di piccoli messaggi di testo (microblogging), immagini, audio e video, si può garantire un'informazione costante e aggiornata, comunicare ed erogare servizi mirati a particolari fasce d'utenza, accrescere la percezione di vicinanza dell'amministrazione ai cittadini. Sono molti gli strumenti utili a questo scopo che in questo momento il *web* mette a disposizione: *forum, wiki, blog, social network, XML e RSS, podcast*, georeferenziazione (cfr. per le definizioni la Tabella B.2 nel Vademecum 2010 "Indicazioni operative per la costruzione, lo sviluppo e la gestione dei siti web delle PA"). La strategia d'uso degli strumenti del web 2.0, all'interno della comunicazione web delle amministrazioni, deve tenere conto:
- del target di riferimento e quindi del ruolo dell'utenza nella costruzione della conoscenza;
- del contesto organizzativo e dei modelli architetturali in cui verrà implementata.

Nella riprogettazione dei servizi e dei contenuti web in una logica 2.0, si raccomanda quindi di:
- definire l'organizzazione dei contenuti sulla base dei bisogni degli utenti;
- erogare i servizi secondo una logica multi canale e multi dispositivo;
- facilitare l'accesso ai dati e alle informazioni attraverso funzionalità evolute di ricerca e localizzazione.

Sennonché queste linee guida, come detto, sono state sostituite da nuove linee guida dove l'unico riferimento ai social è al paragrafo 4.6 che li cita per "valutarsi la sussistenza di un'idonea base giuridica qualora si intenda utilizzare eventuali elementi di terze parti incorporati sui propri siti web (ad es. … *social plug-in*)". Ed anche se non fosse intervenuta la sostituzione nel luglio 2022, le linee ex art.4 della Direttiva n. 8/2009 del Ministro per la pubblica amministrazione e l'innovazione non sono più valide, essendo in applicazione del Codice dell'Amministrazione Digitale (D.lgs. 7 marzo 2005, n. 82), il cui art. 2, comma 6, che è stato modificato dal Decreto legislativo del 13/12/2017 n. 217 (Pubblicato in Gazzetta Ufficiale n. 9 del 12 gennaio 2018 In vigore dal 27/01/2018) stabilendo che "Le disposizioni del presente Codice non si applicano limitatamente all'esercizio delle attività e funzioni di […], nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile". Così l'unico riferimento normativo specifico ai *social media* non è più riferibile alle situazioni di emergenza.

L'evoluzione della normativa in materia di comunicazione del rischio è partita da un riferimento generico ad un diritto all'informazione dei cittadini sino ad arrivare progressivamente a specificarne i contenuti ed i modi, cercando di coinvolgere nella pianificazione del rischio i cittadini e concedendo ai cittadini anche strumenti procedurali in caso di inattività delle amministrazioni responsabili. Ma, almeno per quanto riguarda la normativa italiana che ignorare quasi completamente il termine social media, in definitiva affronta la comunicazione istituzionale in generale, e d'emergenza in particolare, ancora secondo un'impostazione che nella teoria della comunicazione del rischio viene inquadrata in un modello *top-down*, in cui il flusso delle informazioni scorre in modo unidirezionale dall'alto verso il basso dalle istituzioni e dagli esperti al pubblico, eventualmente con l'intermediazione dei *mass media*. Tale modello viene definito "modello deficitario della comunicazione del rischio", a sua volta derivato dal modello adottato dalla Royal Society nel rapporto *Public Understanding of Sience* indicato con l'acronimo PUS[44]. Un tipo di modalità comunicativa di risposta all'emergenza riconducibile a elementi di carattere tattico riguardanti essenzialmente prescrizioni e consigli di soggetti istituzionali chiamati a fornire

44 Sturloni G., (2006), Le mele di Chernobyl sono buone. Mezzo secolo di rischio tecnologico, Sironi, Milano, 2006.

informazioni al pubblico e a interagire con i media durante l'emergenza[45]. Ma in uno studio sulla comunicazione legata ai terremoti basato su due modelli idealtipici: il modello tradizionale e il modello a rete, si osserva che il modello tradizionale è molto più diffuso di quello a rete e che da un punto di vista quantitativo, le istituzioni tendono a utilizzare i social media per diffondere, piuttosto che per raccogliere, informazioni, mentre i cittadini, d'altro canto, tendono a fare affidamento sui social media più per raccogliere informazioni piuttosto che per condividerle, concludendo che il modello a rete non sia, di per sé, più desiderabile di quello tradizionale ma piuttosto che queste categorie aiutino ad acquisire una comprensione più profonda del fenomeno, mentre una combinazione di modelli è necessaria per una comunicazione più efficace durante e dopo i disastri naturali[46].

2. Società del rischio e comunicazione.

"Il mondo è cambiato. Lo sento nell'acqua, lo sento nella terra, lo avverto nell'aria". Così inizia la trilogia cinematografica di Peter Jackson dedicata al capolavoro fantasy del Professore di lingua e letteratura inglese presso l'università di Oxford. E nell'ormai lontano 1986 quando Ulirch Beck – professore di Sociologia prima presso l'università di Münster e Bamberga, poi presso la Ludwig Maximilians Universität di Monaco di Baviera e la London School of Economics – scrisse "Risikogesellschcaft: Auf dem Weg in eine andere Moderne" ["La società del rischio: in cammino verso una modernità diversa"], divenuto celebre attraverso una traduzione in inglese del 1992 con il titolo "Risk Society Towards New Modernity"[47] ["La società del rischio verso una nuova modernità"] doveva avere il sapore un po' Fantasy come dell'*incipit* del Signore degli Anelli sopra ricordato. Il tempo si è preso cura di validare e rendere drammaticamente reali molte delle previsioni e affermazioni del Prof. Beck, a cominciare dal più grande incidente nucleare civile della storia, accaduto a Chernobyl proprio nel 1986. Il libro di Beck è stato così profetico che ha avviato un settore della sociologia del rischio che va da Antony Giddens[48] a Niklas Luhmann [49], da David Le Breton[50] a Zygmunt Bauman[51] e che ha come oggetto di indagine le implicazioni politiche e sociali del rischio, le sue emergenze, il suo controllo e prevenzione nonché la sua percezione.
Secondo Beck non viviamo in una società più rischiosa rispetto alle precedenti per un aumento dei rischi ma per una trasformazione qualitativa dei rischi: "La differenza decisiva *tra rischi classici e quelli moderni* si colloca su un altro piano.

I rischi che nascono dalle tecnologie industriali e dalle grandi tecnologie sono il risultato di decisioni consapevoli - decisioni che vengono prese, da un lato nel quadro di organizzazioni private e/o statali, per conseguire vantaggi economici e cogliere e

45 Coombs W.T., Holladay S.J., (a cura di) (2010), The Hanbook of Crisis Communication, Wiley-Blackwell, Chicester.

46 Comunello F., Mulargia S., (2018), Social Media in Earthquake-Related Communication. Emerald Publishing Limited 2018.

47 Beck U. (1986), *Risikogesellschcaft: Auf dem Weg in eine andere Moderne*, Suhrkamp Verlag, Frankfurt am Main; traduzione inglese del 1992 con il titolo: *Risk Society Towards New Modernity*, SAGE Publications Ltd, California. Successivamente tradotto e pubblicato in italiano da Carocci Editore nel 2000 con il titolo "La società del rischio. Verso una seconda modernità."

48 Giddens A. (1990) The Consequences of Modernity, Polity Press, Cambridge, traduzione italiana: "Le conseguenze della Modernità", Il Mulino, Bologna1994.

49 N. Luhmann (1991), Soziologie des Risikos, Walter de Gruyter & Co., Berlin, traduzione italiana: "Sociologia del rischio", Bruno Mondadori 1996

50 Le Breton D. (1995), *Sociologie du risque*, Presses Universitaires de France, Paris, traduzione italiana Sociologia del rischio, Mimesis Edizioni, Milano, 2017.

51 Bauman Z. (1999) *In Search of Politics*, Stanford University Press, traduzione italiana: "La solitudine del cittadino globale", Feltrinelli, Milano 2000.

corrispondenti opportunità; e, dall'altro, sono adottate sulla base di un calcolo nel quale i pericoli sono considerati come l'inevitabile lato oscuro del progresso. Perciò, questi pericoli legati all'industrializzazione diventano fattore politico non grazie alle loro dimensioni, ma in forza di un carattere sociale: essi non ci travolgono come un destino, ma sono creati da noi, sono un prodotto uscito dalle mani e dalla testa dell'uomo, generato dalla connessione fra sapere tecnico e calcolo dei vantaggi economici"[52]. In altre parole, mentre nella cultura pre-moderna i pericoli e le paure venivano maggiormente attribuite agli dèi o alla natura, e le promesse istituzionali di modernizzazione, come il potenziamento dei mercati, della scienza e della tecnologia, erano considerate la soluzione per condizioni di vita più sicure, oggi invece, i rischi e le minacce vengono attribuite quasi esclusivamente al progresso e alla modernizzazione, a tal punto che fenomeni come il cambiamento climatico, il terrorismo e i disastri ecologici, ci appaiono sempre di più la conseguenza dell'agire umano.

Citando il saggio di Sigmund Freud *Das Unbehagen in der Kultur*, in cui lo psicoanalista austriaco sostiene che la civiltà è frutto di uno scambio tra restrizioni alla libertà individuale in favore della sicurezza, Buaman afferma che se Freud avesse scritto oggi il suo saggio "probabilmente avrebbe dovuto capovolgere la sua diagnosi: […] è la sicurezza a essere sacrificata giorno dopo giorno sull'altare di una libertà individuale in continua espansione.

Mentre inseguivamo qualunque cosa sembrasse aumentare la libertà individuale di scelta e di espressione, abbiamo perduto buona parte della sicurezza ricevuta dalla civiltà moderna, e una parte anche maggiore della sicurezza che aveva promesso di offrirci; ancora peggio, non sentiamo quasi più promettere che quel bene sarà recuperato, mentre sentiamo sempre più spesso che la sicurezza non va d'accordo con la dignità umana"[53].

In questo contesto di perdita della sicurezza, in cui la proliferazione dei rischi è funzionalmente connessa alla promozione della modernità, i rischi hanno perso la loro oggettività, come spiega Beck: "gli analisti del rischio sanno benissimo che *il rischio non è una grandezza misurabile in termini oggettivi*. Cosa significa, allora, «realtà» del rischio? La realtà del rischio si manifesta nel fatto che il rischio venga discusso. I rischi non hanno un'astratta esistenza per sé stessi. *Essi diventano reali nella contraddittoria valutazione di singoli gruppi e popolazioni*. L'idea di un criterio oggettivo in base al quale può essere commisurata la rischiosità trascura il fatto che solo in conseguenza di una determinata percezione e valutazione culturale i rischi sono considerati urgenti, pericolosi e reali o trascurabili e irreali. Ovunque sono in agguato dei rischi. Alcuni vengono tollerati, altri no. Se certi rischi non vengono accettati, non è perché sono più pericolosi di altri? No di certo. Se non lo sono è perché lo stesso rischio a uno sembra un drago, a un altro un lombrico. I rischi accettabili sono i rischi accettati. Questa apparente tautologia ci porta al cuore della questione: quanto maggiore e quanto più oggettivo appare un rischio, tanto più la sua realtà dipende dalla sua valutazione culturale. In altri termini**,** *l'oggettività di un rischio è il prodotto della sua percezione e della sua (anche materiale) messa in scena*"[54]; "*I rischi sono costruzioni e definizioni sociali* sullo sfondo di corrispondenti rapporti di definizione. Essi *esistono nella forma di un sapere* (*scientifico e alternativo alla scienza ufficiale*). Di conseguenza, la loro «realtà» può essere drammatizzata o minimizzata, trasformata o semplicemente negata in conformità delle norme in base alle quali si decide del sapere o del non-sapere. Sono prodotti di lotte e conflitti per le definizioni nel quadro di determinati rapporti di definizione, cioè *risultati di messe in scena* (più o meno riuscite)"[55].

52 Beck U. (2007), *Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit*, trad. It.: "*Contitio humana* Il rischio nell'età globale", Mondadori, Milano, 2023, p.44.
53 Bauman Z. (1999), trad. italiana p.24.
54 Beck U. (2007), *Weltrisikogesellschaft…,* trad. It.: "*Contitio…* ", 2023, p.24.
55 *Ibidem*, p52.

Inoltre in un'ottica luhmanniana, che distingue tra «rischio», dove il potenziale danno futuro dipende da decisioni proprie del decisore, e «pericolo», dove il potenziale danno deriva da decisioni altrui, rileva Umberto Pagano che "Il problema fondamentale è che in molte situazioni gli individui su cui grava il danno potenziale percepiscono il relativo evento come pericolo, mentre i *decision makers* percepiscono lo stesso evento come rischio" e di conseguenza "I rischi dei decisori non sono, quindi, gli stessi di coloro su cui grava l'evento, ma sono rischi loro propri", pertanto "la strategia per minimizzare tale rischio può essere quella di massimizzare l'accettazione contestuale delle decisioni, di renderle «socialmente condivise». Tale strategia implica la creazione in un clima di credibilità e fiducia e si basa, inevitabilmente, su logiche di efficacia comunicativa", dove "gli stessi livelli tecnici e scientifici, poi, non sono affatto immuni da pressioni e ingerenze esterne e spesso non godono l'autonomia e la serenità di giudizio che sarebbero auspicabili" e in definitiva "la comunicazione è un fenomeno che interessa trasversalmente il processo di gestione del rischio", che a sua volta "si configura come un complesso fenomeno sociale basato su processi ermeneutici e comunicativi"[56].

Da quanto sopra il *rischio* (R) non può essere è ricondotto, come vorrebbe la *risk analysis*, solamente alla sua accezione tecnica generale, ossia ad una formula matematica, come prodotto di due fattori R=P x D: dove (P) è la *pericolosità*, consistente nella probabilità che un evento si verifichi in un dato periodo di tempo, e (D) è il *danno*, ovvero l'entità del danno causato. Il rischio non è neppure riconducibile all'accezione proposta dalle Nazioni Unite per le calamità naturali, come il prodotto di tre fattori R=P x V x E: dove (P) è sempre la *pericolosità*, consistente nella probabilità espressa in termini di frequenza del numero di volte in cui l'evento può verificarsi in un dato periodo, (V) è la *vulnerabilità*, che indica la predisposizione a subire un danno degli elementi esposti al pericolo, ed (E) è l'*esposizione*, che consiste nella stima del valore degli elementi esposti al pericolo, sia in termini di vite umane che economici. Ma la cosiddetta valutazione tecnica del rischio (quella che gli anglosassoni chiamano *risk assessment*), va ricompresa nel più ampio concetto di gestione del rischio (in inglese *risk management*) assieme alla sua comunicazione (in inglese *risk comunication*) che consiste nel comunicare gli esiti delle valutazioni degli esperti del rischio al pubblico, coinvolgendolo in un confronto sugli impatti sociali dei rischi[57]. In altri termini analisi e comunicazione sono ontologicamente legati al concetto di rischio.

3. Comunicazione e Social media.

Nell'ormai lontano 1996 nella sua imponente opera il sociologo Manuel Castells[58] partendo dal diffondersi negli anni Ottanta di Internet e del World Wide Web come un potentissimo mezzo di comunicazione e come eccezionale deposito di informazioni e di conoscenza, osservava che nell'Età dell'informazione i processi dominanti sono sempre più strutturati intorno al concetto di rete e giungeva a qualificare la società contemporanea come una vera e propria network society: *una società in rete*. Nel 2012 il sociologo Giovanni Boccia Artieri descriveva il mutamento avvenuto nella società della comunicazione cogliendone un ulteriore aspetto: "Il paradigma comunicativo è mutato. *Il cittadino, infatti, non è più solo oggetto, ma anche soggetto di comunicazione*. Cambia il nostro senso della posizione della

56 Pagano U. (2001), La comunicazione nelle situazioni di rischio, in Quaderni di Sociologia 25/2001, pp.109-110.

57 Sturloni G., (2018), La comunicazione del rischio per la salute e per l'ambiente, Mondadori, Milano, pp.5-8.

58 Castells M.,(1996-1998): The information age. Economy, society and culture: Volume I, The rise of the network society (1996); Volume II, The power of identity (1997); Volume III: End of millennium (1998). I tre volumi sono stati tradotti in italiano dalla Università Bocconi Editore con i titoli di La nascita della società in rete (2002); Il potere delle identità (2003); Volgere di Millennio (2003).

comunicazione: nei *blog*, nei siti di *social network*, costruiamo la nostra riflessività connessa e da lì produciamo, distribuiamo, consumiamo in modi diversi le forme simboliche e i significati che ci servono per abitare il mondo. Quello che stiamo costruendo è un equilibrio sociale diverso. In discontinuità con le categorie conoscitive della modernità. Ne siamo consapevoli solo parzialmente"[59]. Un equilibrio in perenne tensione: dall'avvento di Internet al Web 2.0 siamo diventati cittadini di due mondi: quello online e l'altro offline, diversi, tanto diversi, l'uno dall'altro. Un paradosso dove la rete e i social network hanno bandito la solitudine in un mondo che tende sempre più all'individualismo, realizzando quella "Solitudine del cittadino globale" efficacemente descritta da Zygmut Bauman[60].

I *Social Netwok Sites* (SNS) si sono evoluti e trasformati nel tempo: da piattaforme *statiche*, focalizzate sulla costruzione di un profilo personale e sulla creazione e sostegno di legami sociali per la maggior parte preesistenti nella vita *offline*, a piattaforme *dinamiche*, focalizzate sulla condivisione dei cosiddetti *User Generated content* (UGC), contenuti di varia natura prodotti, postati e liberamente condivisi dagli utenti[61]. A questa trasformazione dei social si accompagna ben presto l'ingresso e la diffusione e dei cosiddetti *Professionally Generated Content* (PGC), contenuti generati non dagli utenti ma da professionisti, ben rappresentato dall'evoluzione di *Twitter*, dove il 10% degli iscritti genera il 90% dei tweet[62], o di *YouTube*, dove il 30% dei video prodotti ogni giorno raccoglie il 90% delle visualizzazioni[63]. Attraverso una fase di *consolidamento* di modelli, diversificazione di strategie e concentrazione di operatori, ed una fase di *co-evoluzione*, in cui le piattaforme collaborano e competono in relazione all'evoluzione dell'intero sistema, configurandosi come strumenti della narrazione della realtà degli eventi[64], i social diventano sempre più piattaforme editoriali[65], dove l'attività di creazione e comunicazione di contenuti è il centro dell'attività mentre la socialità ne è solo un effetto secondario: da *social network* a *social media* si trasformano infine in *media connettivi* [66], dove la socialità è il risultato dell'interazione tra utenti e tra utenti e logiche e interfacce delle piattaforme, e dove "le norme della socialità online sono cambiate […] e sono in divenire. I modelli di comportamento che esistevano nella socialità offline sono sempre più mescolati con le regole sociali e socio-tecniche create nello spazio virtuale"[67]. Tali modelli di comportamento sono ormai così inestricabilmente collegati da dover coniare un nuovo termine *Onlife*, creato dal filosofo Luciano Floridi giocando sui termini online ('in linea') e offline ('non in linea'): *Onlife* è quanto accade e si fa mentre la vita scorre, restando collegati a dispositivi interattivi, in cui la pervasività delle ICT le rende delle vere e proprie "forze sociali" che impattano in maniera radicale sulla nostra stessa concezione di "chi siamo" e sul nostro modo di concepire e relazionarci con la realtà circostante sino a offuscare distinzione tra reale e virtuale e a far venir meno le distinzione tra uomo, macchina e natura, passando

59 Boccia Artieri G., (2012), Stati di Connessione. Pubblici, cittadini e consumatori nella (Social) Network Society, Franco Angeli, Milano.
60 Bauman Z. (1999),op.cit.
61 Vittadini N., (2018), Social Media Studies,Franco Angeli, Milano,pp.35-36.
62 Heil B., Piskorski M., (2009), *New Twitter Research: Men follow men and nobody tweets*, in Harvard Business Review Blog: https://hbr.org/2009/06/new-twitter-research-men-follo
63 Vittadini N., (2018), op.cit., p.68.
64 *Ibidem*, P.51.
65 Van Dijck J., (2013), *Facebook and Engineering of Coonectivity: A multi-layered approach to social media platforms*, in "*Convergence*", vol.19, n. 2, pp.141-155, p.142.
66 Van Dijck J., (2013), *The Culture of Connectivity. A Critical History of Social Media*, Oxford University Press, New York.
67 Van Dijck J., Poell T. (2013), *Understanding Social Media logic*, in "*Media and Comunication*", vol. 1, n.1, p.2-14.

da una condizione di scarsità di informazioni ad una di abbondanza e dai concetti di proprietà e relazioni binarie a quelli di processi e reti[68].

Un altro aspetto fondamentale nella comunicazione attraverso i social media, che ha ripercussioni anche nella comunicazione d'emergenza, è il meccanismo della condivisione dei contenuti. Una frase ormai diventata icastica e straordinariamente efficace per descrivere il fenomeno è: "Se non si diffonde, è morto" (If it doesn't spread, it's dead)[69]. Tenendo presente che per descrivere le forme di partecipazione all'interno dei social media si cita come norma la regola dell'1%[70] che asserisce che il numero di persone che creano attivamente contenuti sul web (UGC), sono circa l'1% del totale delle persone che usufruiranno di quel materiale, si può dire che il *social sharing*, ovvero l'attività di ridistribuzione di contenuti altrui, sia una delle attività principali all'interno dei *social media*. Anzi, considerato che vi è una spinta verso tale attività con la presenza delle icone di condivisione e con gli algoritmi che regolano la visualizzazione dei post e tweet sulle pagine degli utenti anche in base al numero di condivisioni, la condivisibilità delle informazioni è "un elemento strutturale delle architetture di rete"[71]. Di conseguenza "per rimanere *social* […], gli individui devono prendere decisioni cruciali su come condividere le informazioni in ambienti di rete che prosperano sulla condivisione"[72] in tempi stretti, dato che i contenuti nei *social* hanno vita breve, sulla base non di valutazioni complesse, ma in base al numero di *like* che un *post* riceve[73]. Inoltre è ormai assodato che in rete "le persone si connettono tra persone simili", e che quindi "non è facile ottenere l'accesso alle visualizzazioni di persone che pensano da una prospettiva diversa" [74], dando luogo a quel fenomeno chiamato *omofilia delle reti*: nei *social* la credibilità di un contenuto viene attribuita non per la validità della fonte ma attraverso una catena di fiducia tra amici di amici, definita FOAF (*Friend of a friend*), che spesso hanno le medesime posizioni così creando le cosiddette *echo chamber*[75], dove risuonano come un eco le stesse opinioni. Tale situazione è poi aggravata dagli algoritmi che selezionando le visualizzazioni dei contenuti in base ai comportamenti precedenti dell'utente finiscono per collocarlo in una sorta di bolla informativa, definita *filter bubble*[76], sino a generare fenomeni di radicalizzazione[77]. La sociologa Nicoletta Vittadini, citando un caso avvenuto in Texas, spiega che questo tipo di fenomeni genera una divergenza tra i flussi di comunicazione: un *tweet* contenente un'informazione falsa raggiunge i 16.000 *retweet* e su *Facebook* viene

68 Floridi L., (a cura di), (2015), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Springer, New York- London.

69 Jenkis H., Ford S., Green J., (2013), Spreadable media: creating value and meaning in a network culture, NYU Press, New York, p.1.

70 La regola dell'1% è stata coniata nel maggio del 2006 dai blogger Ben McConnell e Jackie Huba: The 1% Rule: Charting citizen participation, su churchofthecustomer.com. URL consultato il 16 aprile 2011 (archiviato dall'url originale l'11 maggio 2010).

71 Papacharissi Z., Gibson P. L., (2011), *Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites*, in: Trepte, S., Reinecke, L. (eds) "Privacy Online", Springer, Berlin, Heidelberg, p. 76.

72 *Ibidem*.

73 Van Dijck J., Poell T., (2013), *Understanding Social Media Logic*, in "Media and Communication", 2013, Vol.1, n.1, pp. 2-14

74 boyd d., (2010) Streams of Content, Limited Attention: The Flow of Information through Social Media, in Web2.0 Expo. New York, NY: November 17, testo disponibile online: https://www.danah.org/papers/talks/Web2Expo.html

75 Jamieson, K., Cappella, J., (2009), *Echo Chamber: Rush Limbaugh and the Conservative Media Establishment*, Oxford University Press; Sunstein, C. R. (2017), #Republic: Divided Democracy in The Age of Social Media, Princeton University Press.

76 Pariser E., (2011), The Filter Bubble: What the Internet Is Hiding from You, Penguin Group, New York.

77 Anzera G., Massa A., (2021), Chi ha paura di Internet? Le piattaforme online nei processi di radicalizzazione e di deradicalizzazione, Franco Angeli, Milano.

condiviso 350.000 volte, mentre il *tweet* di rettifica, contenente l'informazione corretta, raggiunge 254 *like* e 27 *retweet*; tale enorme divario della diffusione tra la notizia falsa e la sua rettifica è dovuto proprio al fatto che le due informazioni corrono su reti differenti, la falsa in reti omofile dove il meccanismo FOAF fa da volano alla sua diffusione, mentre la notizia vera circola assai di meno su reti *mainstream*, "in competizione con la fiducia relazionale e affettiva dei social media"[78].

4. Comunicazione d'emergenza e social media e algoritmi.

In questo quadro si inserisce la comunicazione d'emergenza, che consiste in un processo di acquisizione e diffusione di informazioni per contrastare un evento emergenziale allo scopo di incrementare il livello organizzativo del sistema e di ridurne il livello di imprevedibilità[79]. È necessario fare una distinzione concettuale tra disastro, emergenza e crisi. Disastro è un evento imprevisto e improvviso che provoca un'emergenza, che invece si configura come "un processo in cui le routine del sistema colpito […] sono sconvolte e richiamano i diversi attori a compiti non ordinari"; mentre in passato la riflessione scientifica limitava il concetto di emergenza ai soli eventi catastrofici naturali, oggi si parla di crisi come di "un processo con le caratteristiche dell'emergenza, ma generalmente prescindendo dalle sue cause" [80].

Comunque le definizioni di emergenza sinora elaborate sono due: una *frequentista* e l'altra *cognitiva*.

La prima fa riferimento alla frequenza del verificarsi di un evento, dove ad un alto grado di frequenza corrisponde la normalità, mentre ad un basso grado di frequenza corrisponde la non normalità, quindi l'emergenza. Invece la *definizione cognitiva di emergenza*, parte dal presupposto che la sopravvivenza dipende dalla prevedibilità o meno dell'ambiente in cui si vive, e ritiene quindi necessario "dominare la variabilità ambientale da parte del sistema socio-culturale, con i suoi mezzi conoscitivi e tecnologici, per cercare di ridurre, all'interno dell'insieme normalità, anche gli eventi classificati come rari, secondo la loro frequenza: conoscere, prevedere approntare strategie non riduce la probabilità del verificarsi della calamità, ma riduce enormemente il danno"[81]. Tale definizione di emergenza ha il pregio di collocare il concetto di vulnerabilità non nell'emergenza ma nel sistema nel suo complesso, o meglio nella *subcultura dell'emergenza*, che consiste nel grado di cultura specifico posseduto da ciascun sistema di reagire a quell'evento, dando così ragione del caso di due sistemi sociali colpiti da eventi di pari intensità, ma con effetti dannosi differenti[82]. In altri termini gli effetti della crisi sono già contenuti dentro al sistema colpito, che rivela una maggiore vulnerabilità rispetto ad un altro: "la definizione cognitiva dell'emergenza insieme al concetto di vulnerabilità, hanno il pregio, e la responsabilità, togliere all'evento scatenante la crisi i connotati della fatalità ineluttabile e di collocare le strategie di gestione dell'emergenza nell'insieme di quelle socialmente necessarie per governare i processi di sviluppo e mutamento del sistema sociale. In questa prospettiva concettuale la prevenzione diventa un dovere sociale"[83].

78 Vittadini N., (2018), Op. cit., p.125.
79Coombs, W. T., (2007), Ongoing Crisis Communication: Planning, Managing, and Responding, SAGE, Los Angles.
80 Lombardi M., (2005), Comunicare nell'Emergenza, Vita e Pensiero, Milano, p.27.
81 Ibidem, p.29.
82 Quantarelli E.L., (a cura di), (1978), *Disaster: Theory and Research, Sage*, California, 1978.
83 Lombardi M., (2005), Op. cit., p.32.

Per quanto sopra appare evidente che la comunicazione d'emergenza non può riguardare la sola fase emergenziale ma ricomprende riguarda le fasi precedenti l'evento emergenziale, la fase di emergenza vera e propria ed infine la fase post emergenza.

Gli obiettivi della comunicazione durante la *fase pre-emergenza*, detta anche *care comunication*, si possono sintetizzare in:
- prevenire quanto più possibile il rischio;
- informare su come gestirlo;
- sensibilizzare per minimizzarlo.

Tale attività ricomprende la creazione di strumenti da utilizzare durante l'emergenza, come piani operativi, procedure intra e inter-istituzionali, l'individuazione di canali preferenziali tra i media, l'addestramento dei portavoce e del team di comunicazione. In questa fase per prevenire, informare e sensibilizzare su come conoscere, gestire e minimizzare il rischio e l'emergenza è necessario:
- preparare dei piani di gestione delle crisi, comprensivi di esercitazioni pratiche e di piani di comunicazione delle crisi che stabiliscano ruoli ben precisi delle diverse parti interessate, le modalità di comunicazione tra di loro e con il pubblico e che prevedano anche l'utilizzo dei i social media;
- fornire informazioni sicure, scientificamente dimostrate in modo comprensibile al pubblico destinatario;
- divulgare i fattori di rischio e i segnali di allertamento relativi ad esso;
- informare sulle azioni da compiere o da non compiere qualora l'emergenza si verifichi.

In sintesi si tratta costruire quella subcultura della crisi che favorisca "il comportamento adattivo durante l'emergenza"[84], una sorta di educazione al rischio[85] per rendere il sistema resiliente.

Successivamente c'è *la fase della comunicazione durante l'emergenza*, detta anche *crisis communication*, dove è indispensabile "un ruolo attivo della popolazione, a cui è richiesto di reagire a una minaccia adottando comportamenti idonei per mettersi in sicurezza, mentre le istituzioni preposte alla gestione del rischio conservano un ruolo di guida, fornendo informazioni e indicazioni comportamentali, presuppone che, per quanto possibile, la consapevolezza del rischio e dei comportamenti da adottare per difendersi – la cd. «cultura del rischio» – sia condivisa prima dell'emergenza, ovvero in «tempo di pace»"[86]. La comunicazione durante la fase dell'emergenza "consiste in quello scambio di messaggi atti ad allertare la popolazione interessata dalla stessa, favorendo una reazione che faciliti il mantenersi al sicuro o mettersi in salvo, o che comunque agevoli il più possibile le operazioni di soccorso"[87], con lo scopo di superare la crisi il più rapidamente possibile per riportare a normalità il sistema. In questa fase i mezzi di comunicazione "giocano un ruolo fondamentale in quanto rispondono al bisogno primario di fornire informazioni e favoriscono il mantenimento dell'equilibrio di ciascun attore coinvolto"[88].

Tale fase emergenziale può essere suddivisa in due sub-fasi:
- la sub-fase relativa alla gestione iniziale dell'emergenza, in cui sono essenziali la semplicità, la credibilità, la coerenza, la verificabilità e la velocità delle informazioni, in modo da accreditare sin dal primo momento le istituzioni impegnate nella gestione dell'emergenza,

84 Lombardi M., (2005), Op. cit., p.83.
85 Zuccaro A., (2021), La comunicazione nella gestione delle emergenze, Palermo, p.27.
86 Sturloni G., (2018), Op. cit., p.91.
87 Zuccaro A., (2021), op. cit., p.65.
88 Lombardi M., (2005), Op. cit., p.65.

quale principale fonte di informazioni e così limitare la diffusione incontrollata di voci e di *rumors*;
- la sub-fase relativa al mantenimento dei soccorsi, in cui, aumentando le informazioni rispetto alle diverse esigenze, è necessario da un lato, aiutare la popolazione coinvolta a comprendere meglio la situazione, e dall'altro, supportare i soggetti non direttamente colpiti verso le operazioni di gestione dell'emergenza, sia con campagne di sensibilizzazione che con informazioni dettagliate su come aiutare concretamente i soggetti coinvolti[89].

Infine c'è la fase post-emergenza che può essere suddivisa a sua volta in due sub-fasi:

- la sub-fase *della risoluzione*, che ha inizio quando la gestione dell'emergenza sta per essere definitivamente portata a termine, durante la quale è importante trarre delle prime conclusioni rispetto a quanto ha funzionato e dove i soccorsi si sono mostrati maggiormente carenti, ed è altrettanto importante rafforzare i messaggi di prevenzione spiegando come comportarsi durante la normalità per ridurre il rischio e come agire nel caso l'emergenza si ripresenti;

- la sub-fase *della valutazione*, quando l'emergenza è definitivamente superata, in cui si fa il punto della situazione ed in particolare si valuta la performance della comunicazione per capire cosa abbia funzionato e cosa invece ha creato difficoltà.

In definitiva la fase post-emergenziale non è solo il momento in cui si fa tesoro delle esperienze apprese durante la crisi, ma anche il periodo, di lunghezza variabile, di gestione degli effetti dell'emergenza, come ad esempio nel caso si siano verificate vittime, dove momenti di commemorazione e ricordo negli anni a seguire prolungano questa fase della comunicazione di emergenza e contribuiscono a rafforzare la legittimazione e la fiducia dell'istituzione che ha gestito l'emergenza[90]. In questa fase ad esempio ha un ruolo importantissimo la Psicologia dell'emergenza, che nella cultura statunitense viene definita *disaster psycology*, che si occupa delle conseguenze psicologiche sia individuali che sociali delle situazioni emergenziali: "ancor più catastrofico del sisma è quel terremoto che né si vede né si ode, quel terremoto che avviene dentro"[91]. È bene ricordare che le vittime di un'emergenza non sono solo coloro che subiscono in via diretta l'impatto dell'evento ma potenzialmente una tutta serie di persone così individuate e classificate dallo psicologo Taylor e dallo psichiatra Frazer Victoria University di Wllington[92]:

1. Vittime di primo livello chi subisce in via diretta l'impatto dell'evento catastrofico
2. Vittime di secondo livello parenti e amici delle vittime di primo livello
3.Vittime di terzo livello personale di soccorso
4. Vittime di quarto livello la comunità coinvolta nel disastro e chi, in qualche modo, ne è eventualmente responsabile
5. Vittime di quinto livello

89 Anzera G., (2014), "La comunicazione d'emergenza nel conteso contemporaneo", in Comunello F. (a cura di), (2014), Social Media e Comunicazione d'Emergenza, Milano, pp.21-22.
90 Ibidem, p.23.
91 Petrone L., (2002), Emergenza in Italia, in Iacono A. e Troiano M., (a cura di), (2002), Psicologi dell'emergenza, Editori Riuniti, Roma, pp.75-76.
92 Frazer, A.G & Taylor, A.J.W. (1981), *Psychological sequelae of Operation Overdue following the DC10 aircrash in Antartica*, in Psychology, No.27., 72.

individui il cui equilibrio psichico è tale che, anche se non sono coinvolti direttamente nel disastro, possono reagire con un disturbo emozionale
6. Vittime di sesto livello individui che, per un diverso concorso di circostanze, avrebbero potuto essere loro stessi vittime di primo livello o che hanno spinto altri nella situazione della calamità o che si sentono coinvolti per altri motivi indiretti

Questa attività rivolta alle vittime di un'emergenza consiste in un lungo processo di recupero, ricostruzione e ristabilimento, che consente di attivare due risorse psicologiche definite coping e resilienza, che si articola in una serie di tecniche, come il debriefing e il defusing, inquadrate e classificate da Everly G. e Mitchell L. nel Critical Incident Stress Management[93]. Un altro compito particolarmente complesso della comunicazione post emergenziale riguarda il caso in cui si siano verificati rapporti problematici con i media o con il pubblico durante la crisi che siano arrivati ad incrinare il rapporto di fiducia tra media, pubblico e istituzioni. Si tratta di un lavoro solitamente molto lungo e indispensabile, perché senza il rispetto dei ruoli e la stima tra interlocutori, qualsiasi messaggio perde valore e in definitiva ogni tipo di comunicazione è vana. Ad esempio i social media possono essere fondamentali nelle fasi successive all'emergenza nel fornire uno spazio per la ricostruzione delle relazioni sociali, per la condivisione delle esperienze, per l'espressione del lutto e della solidarietà, per la costruzione collaborativa della memoria[94].

In generale è bene precisare che la comunicazione post emergenza più che mirare a recuperare la normalità che precedeva la crisi, punta a creare un nuova normalità, tenendo conto in modo oggettivo di tutti i parametri della comunicazione, dai dati del traffico comunicativo, ai commenti e condivisioni sui differenti canali sino agli elementi umorali, con l'obiettivo sia di educare alla nuova normalità, attraverso la formazione e la modifica dei propri atteggiamenti, sia di creare una memoria storica che dia nel rispetto dei ruoli e delle vittime una visione il più possibile veritiera dell'accaduto con un approccio cronachistico per non dare spazio a *fake news* e *rumors*, che potrebbero in seguito rivelarsi fonte di delegittimazione delle istituzioni[95]. Per concludere è importante avere chiaro che le fasi della comunicazione pre e post emergenza sono strettamente connesse: un sistema è tanto più preparato a gestire un'emergenza quanto più saprà trarre insegnamenti dagli eventi favorevoli o sfavorevoli al superamento della stessa.

Per pianificare una comunicazione d'emergenza è necessario agire come per qualsiasi altro tipo di comunicazione e quindi confrontarsi con questi quattro aspetti:

1. definire i propri obiettivi;
2. conoscere il profilo dei destinatari;
3. individuare i canali di comunicazione più adatti;
4. scegliere i messaggi.

Il primo passo può sembrare scontato, ma dato che la comunicazione d'emergenza deve stimolare una risposta di tipo adattativo dei propri interlocutori, diventa essenziale avere ben chiari quali tipo di cambiamenti si vuole ottenere da loro.

Il secondo passo è altrettanto basilare ma di fondamentale importanza per raggiungere l'obiettivo: spesso ci si dimentica che non si sta solo comunicando qualcosa, ma che si sta

93 Mitchell J.T. and Everly G.S. (1997) Critical Incident Stress Management: a new era and standard of care in crisis intervention, Ellicott City, MD.: ed.Chevron Publishing Corporation.
94 Farinosi M., Micalizzi A., (a cura di), (2013), Netquake. Media digitali e disastri naturali, franco Angeli, Milano.
95 Zuccaro A., (2021), op. cit., pp.139-144.

comunicando con qualcuno[96]. Quindi se non si vuol rischiare di essere ignorati, si deve conoscere il profilo dei destinatari a cui ci si rivolge e si deve instaurare una relazione di fiducia tra chi comunica e chi riceve il messaggio. E ciò ancor più nei social, dove uno degli scopi prioritari non è l'informazione, come nei media tradizionali, ma la costruzione di relazioni significative: presentarsi con autorevolezza e professionalità e coltivare un dialogo ascoltando il proprio interlocutore è forse più importante del messaggio stesso[97]. Sui differenti tipi di audience è ancora valida la segmentazione dei pubblici fatta dallo studioso della comunicazione d'emergenza Grunig[98], che ha individuato quattro gruppi: il primo, detto "*no public*" , composto dai soggetti che non comprendono la gravità della situazione e sottovalutano i messaggi; il secondo, definito "pubblico latente", che riguarda il gruppo sociale potenzialmente coinvolto nell'evento e a rischio di subirne gli effetti, ma non ancora consapevole del contesto; il terzo gruppo composto dal "pubblico consapevole", che comprende la portata dell'emergenza e che esige informazioni e direttive da parte delle istituzioni; ed infine il quarto gruppo, che è quello direttamente collegato alla gestione dell'emergenza che va informato sul campo delle procedure da seguire per essere di supporto ai soggetti coinvolti.

Il punto è che i vari pubblici si presentano tutti insieme nello stesso momento e richiedono contemporaneamente diversi messaggi informativi: ad esempio, bisognerà convincere il *no public* della gravità della situazione, mentre il pubblico consapevole andrà informato correttamente sulle procedure da seguire e così via[99].

Il terzo passo è la scelta dei canali di comunicazione, che si possono suddividere in base al numero di soggetti coinvolti nella comunicazione in quattro modelli comunicativi:

a) I mezzi di comunicazione *broadcast*, utilizzati dalle istituzioni per comunicare con i cittadini in maniera indifferenziata e sono la televisione, la radio, i giornali ed i siti web;
b) I mezzi di comunicazione *one to one* unidirezionali, utilizzati dalle istituzioni per comunicare con i cittadini ma in maniera differenziata e sono e-mail (newsletter), sms, e telefonate;
c) I mezzi di comunicazione *one to one* bidirezionali, utilizzati sia dalle istituzioni che dai cittadini per mettersi in contatto con le istituzioni e sono sempre email e telefono spesso gestiti da un unico contact center;
d) I mezzi di comunicazione *many to many*, utilizzati principalmente dai cittadini per comunicare tra loro e dalle istituzioni sinora in modo tendenzialmente unidirezionale secondo un modello top-down. Si tratta ovviamente dei social media, come ad esempio Twitter (ora X) e Facebook.

La scelta dei canali è strettamente collegata al passo precedente perché ad ogni pubblico corrisponde un tipo di media. Così ad esempio per rivolgersi ad un pubblico in generale, si utilizzeranno i media tradizionali, a cui si rivolgono e il 74,1% degli italiani[100], mentre se si vogliono raggiungere più selettivamente i diversi pubblici ci si rivolgerà ai social media, avendo presente che Il 64,3% degli italiani dichiara di utilizzare un mix di fonti informative, tradizionali e online; c'è poi un 9,9% che attinge solo ai media tradizionali e un 19,2%, poco meno di 10 milioni di italiani in valore assoluto, che si affida esclusivamente alle fonti online[101]. Rimanendo nei social media la scelta va ulteriormente selezionata in base al pubblico: Twitter (X) rappresenta quello più vicino alla funzione giornalistica, mentre

96 Carrada Giovanni, (2005), Comunicare la scienza, Sironi, Milano.
97 Zuccaro A., (2021), op. cit., p.126.
98 Grunig J., (2013), Excellence in Public Relations and Communication Management, Routledge.
99 Anzera G., (2014), op. cit., p.20.
100 Rapporto CENSIS 2023, reperibile online: https://www.censis.it/comunicazione/il-vero-e-il-falso-0
101 Ibidem.

Facebook è più generalista per un'utenza sopra i trent'anni, Instagram tra i 20 e i 40, TikTok tra le fasce più giovani[102]. Inoltre la scelta dei canali è influenzata anche dal primo passo, ovvero gli obiettivi da raggiungere, secondo una suddivisione ben schematizzata nella tabella[103] qui di seguito:

Tipologia di obiettivo	Tempistiche dei risultati	Canali privilegiati
Informazione	Breve termine	Mass media
Educazione	Lungo termine	Scuole, e-learning
Persuasione	Breve/medio termine	Pubblicità, attività di lobbying
Coinvolgimento	Medio termine	Comunicazione interpersonale Campagne, social media
Mobilitazione	Breve/medio termine	Canali privilegiati

Infine il quarto passo che riguarda la scelta dei messaggi. Qui per quanto riguarda i social media è necessario fare una premessa circa l'utilizzo che se ne vuol fare durante tutta la fase emergenziale: "innanzitutto, i social media possono essere utilizzati in modo passivo per diffondere informazioni e ricevere feedback dagli utenti tramite messaggi in arrivo, post in bacheca e sondaggi. Mentre un secondo approccio prevede l'uso sistematico dei social media come strumento di gestione delle emergenze. L'utilizzo sistematico potrebbe includere l'utilizzo del mezzo per condurre comunicazioni di emergenza ed emettere avvisi; utilizzare i social media per ricevere richieste di assistenza da parte delle vittime; monitorare le attività degli utenti per stabilire la consapevolezza situazionale; e utilizzare le immagini caricate per creare stime dei danni, tra le altre cose"[104]. È evidente che cambia il contenuto dei messaggi se si utilizza il primo o il secondo dei due approcci all'utilizzo dei mass media. Poi bisogna distinguere la formulazione dei messaggi con riferimento alla fase dell'emergenza – pre-durante-post – ed in base anche all'oggetto della comunicazione. Ad esempio si pensi alla differenza della comunicazione tra rischio terroristico e ambientale: il primo può far leva direttamente sulle immagini oscene della violenza, mentre il secondo è il "risultato di una messa in scena *top-down*"[105] dovuta ad una comunicazione che comprende un'alleanza di scienziati, politici e movimenti sociali, che necessità un'articolata comunicazione che parta dai media tradizionali, con le loro funzioni di selezione (*gatekeeper*) ed di gerarchizzazione (*agenda setting*) delle informazioni[106], attraverso comunicati stampa, interviste, conferenze, programmi televisivi e radiofonici, e arrivi sino ai nuovi media, per mezzo di newsletter, blog e social media.

I messaggi devono essere innanzitutto tempestivi perché quando un'organizzazione è la prima a segnalare l'emergenza, la sua reputazione subisce meno danni che se qualche fonte esterna, come i mezzi di informazione, sia la prima a segnalare l'esistenza della crisi[107].

102 Zuccaro A., (2021), op. cit., p.125.
103 Sturloni G., (2018), Op. cit., p.50.
104 Lindsay B. R., (2011) *Social Media and Disasters: Current Uses, Future Options, and Policy Considerations*, report, September 6, 2011; Washington D.C.. (https://digital.library.unt.edu/ark:/67531/metadc93902/: accessed March 26, 2024), University of North Texas Libraries, UNT Digital Library, https://digital.library.unt.edu; crediting UNT Libraries Government Documents Department.
105 Beck U. (2007), trad. It, (2023), p.118.
106 Lombardi M., (2005),Op. cit., pp.39-48.
107 Coombs, W.T. (2014), "State of crisis communication: evidence and the bleeding edge", Research Journal of the Institute for Public Relations, Vol. 1 No. 1, pp. 1-12.

Assieme alla tempestività deve esserci la trasparenza: bisogna diffondere le notizie di sui si dispone, ammettendo ciò che si sa e ciò che non si sa, senza balzi in avanti, interpretazioni azzardate o notizie verificate, che in seguito comprometterebbero la fiducia nell'istituzione che le ha comunicate.

Inoltre la comunicazione deve essere comprensibile ai destinatari, perché lo scopo non è trasformare i cittadini in esperti, ma metterli in condizione di gestire le informazioni ricevute per mettersi in salvo e proteggersi dai pericoli. Più in generale nelle fasi pre e post emergenza è necessario fornire codici culturali per dare una corretta interpretazione dell'accaduto ed in seguito suscitare comportamenti proattivi, mentre nella fase dell'emergenza bisogna definire il più possibile nel dettaglio la situazione per orientare i comportamenti. Infatti, poiché i messaggi hanno lo scopo di stimolare una risposta adattativa, devono essere puntuali, coerenti e non problematici sui contenuti, per non lasciare spazio ad ambiguità e fraintendimenti, ed essere attenti ai reali bisogni degli interlocutori, perché principio fondamentale nell'informazione non è fornire dati, ma fornirli in maniera adeguata e congruente alla domanda, seguendo un modello a onde della curva della domanda e della risposta dell'informazione, in modo da ridurre la vulnerabilità del sistema[108]. Così ad esempio durante il terremoto del Friuli del 1976 se descriviamo su un asse temporale le richieste di ammissione dei feriti all'ospedale di Udine, il principale presidio sanitario del territorio, nelle prime ore hanno effettuato un balzo verso l'alto i feriti con traumi, scendendo in seguito a livelli quasi normali in 72 ore dall'impatto, mentre i feriti con problemi medici sono stati la maggioranza in un secondo momento, circa 30-40 ore dopo[109].

È quindi necessario dare precedenza ai messaggi in base alle esigenze manifestate dalla popolazione e adottare un approccio dialogico con gli altri soggetti portatori di interessi e, quando possibile, favorire la partecipazione ai processi decisionali, perché nella gestione dell'emergenza il coinvolgimento del pubblico è essenziale[110]: è prioritario ascoltare i tutti gli *stakeholder*, perché "la prima forma di accoglienza è un ascolto partecipato e partecipativo, in un'ottica dialogica"[111]. Si inserisce in questo contesto anche la scelta nel piano d'emergenza di nominare un'unità di crisi e un portavoce dell'istituzione, atto che consente di "personificare l'istituzione", dandole un volto e una voce[112], perché siamo più disponibili a dare fiducia ad una persona piuttosto che ad una struttura astratta[113].

È fondamentale comprendere che la comunicazione d'emergenza non può essere limitata ad un solo canale e alle norme che lo regolano, ma ognuno di essi fa parte di un'unica comunicazione articolata tra diversi media e diversi *stakeholder*. È ormai assodato che a causa dell'aumento dei servizi di *social networking* (SNS), la comunicazione Internet è un metodo onnipresente per lo scambio di informazioni su una crisi[114]. Ad esempio in Italia si registra ancora un forte aumento dell'impiego di internet da parte degli italiani (l'88% di utenza: +4,5%) e di quanti utilizzano gli *smartphone* (l'88%: +4,7%) e lievitano complessivamente all'82,4% gli utenti dei *social network* (+5,8%), mentre i media tradizionali rimangono molto

108 Lombardi M., (2005),Op. cit., pp.67-71.
109 Ibid. pp. 30-31.
110 Sturloni G., (2018), Op. cit., p.96.
111 Zuccaro A., (2021), op. cit., p.111.
112 Sturloni G., (2018), Op. cit., p.97.
113 Covello et Alii, (2009), Vincent T. Covello, Richard G. Peters,Joseph G. Wojtecki, and Richard C. Hyde, Risk Communication, the West Nile Virus Epidemic, and Bioterrorism: Responding to the Communication Challenges Posed by the Intentional or Unintentional Release of a Pathogen in an Urban Setting, in Journal of Urban Health, Vol. 78,No. 2,June 2001,pp.382-391, p.386.
114 Yi, C.J. and Kuri, M. (2016), The prospect of online communication in the event of a disaster, Journal of Risk Research, Vol. 19 No. 7, pp. 951-963.

forti: la tv nel 2023 a guardarla è complessivamente il 95,9% degli italiani e i radioascoltatori sono il 78,9% degli italiani, con il crollo dei soli quotidiani cartacei venduti in edicola, che nel 2007 erano letti dal 67,0% degli italiani, ridottisi al 22,0% nel 2023 (con una differenza pari a -3,4% in un anno e a -45,0% in quindici anni)[115]. Quindi affinché la comunicazione in caso di crisi sia efficace, gli strumenti dei social media devono far parte delle strategie di comunicazione. Come ad esempio nel caso della mappa Ushahidi, che è stata creata da una società senza scopo di lucro (Ushahidi), spinta da Ory Okolloh, un *blogger* e attivista, che utilizzando il suo *blog* per raccogliere informazioni sugli scoppi di violenza nel periodo post-elettorale del 2007 in Kenya, con l'aiuto di diversi sviluppatori, ha implementato una mappa della crisi *open source* fornendo informazioni alternative a quelle del governo sugli incidenti di violenza. Il successo di questa *crowmap*, *open source* dal 2010, ha dato vita ad un vero e proprio fenomeno di *crsis mapping*, un'attività di raccolta, visualizzazione e analisi dei dati in tempo reale in eventi di crisi dovuti a cause di natura diversa[116], come nel caso del terremoto di Haiti del gennaio 2010, lo tsunami giapponese del 2013, o l'alluvione in Sardegna del novembre 2013[117]. Questo tipo progetti si basa sul lavoro di volontariato di pochi sviluppatori e sul contributo fondamentale della comunità, attraverso la condivisione degli User Generated Content (UGC): l'aggregazione di input co-generati come comunicazioni catturate o comunicazione tramite interne a *social* media sono combinate con dati geo-referenziati e geo-spaziali per creare mappe digitali, il più aggiornate possibile.

La comunicazione d'emergenza attraverso i *social* media durante una crisi dovrebbe essere un processo integrato che offra non solo dati e informazioni ma anche, ad esempio, supporto emotivo[118], perché non si sta solo comunicando qualcosa, ma si sta comunicando con qualcuno. È importante notare che non esistono due crisi completamente identiche e, di conseguenza, nessun piano di comunicazione è applicabile a ogni crisi[119] e che in contesti diversi non esiste un unico tipo di comunicazione sufficiente per tutte le crisi[120]. Bisogna tenere conto anche il *digital divide* durante le catastrofi: ad esempio in un'analisi esplorativa dei dati empirici di un'indagine sulle famiglie sulla ricerca di informazioni, sull'attività di condivisione e sulla percezione dell'affidabilità delle informazioni sulle piattaforme di social media in diversi gruppi di popolazione durante tre importanti uragani negli Stati Uniti tra il 2017 e il 2018. I risultati di questa analisi suggeriscono associazioni significative tra l'uso dei social media e fattori socioeconomici: (1) i fattori socioeconomici insieme agli effetti geografici giocano un ruolo nel determinare non solo l'adozione della piattaforma ma sia le motivazioni per la ricerca di informazioni che l'azione di condivisione delle informazioni sui social media, (2) Il tipo di piattaforma di *social* media influenza il tipo di informazioni che le persone cercano, (3) le famiglie provenienti da contesti socioeconomici inferiori e appartenenti a minoranze erano più propense a utilizzare le piattaforme di social media per cercare informazioni diverse sui *social* media rispetto ai loro pari, (4) la percezione dell'affidabilità delle informazioni è influenzata anche dal divario sociale: le famiglie delle

115 Rapporto CENSIS 2023, cit..

116 Wikipedia, *Crowdmapping*: https://it.wikipedia.org/wiki/Crowdmapping

117 Lovari A., Murtas F., (2014), Comunicazione di crisi e pratiche digitali di engaement: il caso della mappa condivisa SardSos", in Comunello F. (a cura di), (2014), Social Media e Comunicazione d'Emergenza, Milano, pp.141-159.

118 Liu B. F., Austin L., Jin Y., (2011) How publics respond to crisis communication strategies: The interplay of information form and source, Public Relations Review, 37(4), 345-353.

119 Coombs W. T., (2020), Public Sector Crises: Realizations from Covid-19 for Crisis Communication, reperibile online: http://siba-ese.unisalento.it/index.php/paco/article/view/22498

120 Cannaerts N., (2021), Crisis communication in public emergencies: multistakeholders' perspectives, International Journal of Emergency Services, 2021, Vol. 10, n.1.

aree rurali, i gruppi a basso reddito e le minoranze razziali avevano maggiori probabilità di segnalare una maggiore inaffidabilità delle informazioni sui *social* media[121]. Il docente di strategie della Comunicazione di emergenza e fondatore e coordinatore del comitato scientifico di emegenza24, il più importante *network* di emergenza europeo, Maurizio Galluzzo, sostiene che "I temi che riguardano la comunicazione della crisi spesso sono legati a fenomeni complessi in cui ci aiuta di più la teoria del caos che una singola disciplina" e spiega che ad esempio "in condizioni di conversazioni in ambiente ostile per poter essere efficaci servono strategie di comunicazione che non si possono riassumere con un elenco di regole da utilizzare"[122].

Stando ad uno studio sulla comunicazione di crisi e pratiche digitali di *engaement*[123] alla domanda su chi preferiresti fornisse informazioni in una mappa pubblica durante un'emergenza la maggioranza degli intervistati (83%) ha indicato la voce "i cittadini insieme alle amministrazioni e agli enti preposti all'emergenza". Ed in un altro studio alla domanda da quali fonti preferissero per ottenere informazioni di emergenza, i cittadini italiani hanno dato priorità al livello locale, sottolineando anche il ruolo del sindaco[124]. In piena sintonia con la centralità del livello locale del sistema italiano di protezione civile, basato com'è sui Comuni, dove il Sindaco è, per legge, il primo organo di protezione civile e dove il Dipartimento della Protezione Civile (livello statale) viene formalmente attivato dal sindaco, se l'emergenza supera i confini regionali[125]. In altri termini, durante un'emergenza il favore accordato al livello locale più prossimo indica che i cittadini durante un'emergenza cercano persone, il più possibile vicine, che conoscano loro e il territorio, non sono solo dati e informazioni.

La comunicazione d'emergenza è un tipo comunicazione complesso, multidisciplinare e articolato tra diversi *stakeholder*, che non si presta ad una semplice riduzione ad un processo digitale, nemmeno quando si tratta dei nuovi media, perché si compone di relazioni tra istituzioni, esperti, giornalisti, cittadini, in cui i flussi comunicativi *top-down* e *bottom-up* si mescolano, e modelli organizzativi tradizionali si ibridano con le logiche dell'informazione in rete, il cui fondamento è un rapporto personale, un metterci il volto, che vale per i cittadini come per le istituzioni e che mal si concilia con l'idea che al posto delle persone a scrivere e rispondere ci sia un algoritmo di intelligenza artificiale. Il posto corretto degli algoritmi può essere di supporto alla gestione di un'emergenza. Ad esempio guardando ai numeri di uno studio sull'utilizzo in *Twitter* dell'*hashtag* #allertameteoSar durante delle precipitazioni intense in Sardegna, dove il totale dei *Tweet* legati all'*hashtag* è di 93.091 ed il totale dei *tweet* riconducibili alle istituzioni con un account *Twitter*, quello del comune e quello personale del governatore della Sardegna, sono rispettivamente 38 e 33. Si comprende come l'input dei messaggi sia sovrabbondante, mentre output sia piuttosto limitato. In questo contesto l'intelligenza artificiale potrebbe intervenire non tanto per rispondere, quanto per classificare attraverso algoritmi di *clustering* tutti i messaggi in entrata, ad esempio secondo le logiche sopra ricordate del modello a onde della curva della domanda e della risposta dell'informazione[126], mettendo in evidenza le richieste di soccorso ed anche quelle non ben

121 Dargin et al., (2021), Dargin J., Fan C., Mostafavi A., *Vulnerable populations and social media use in disasters: Uncovering the digital divide in three major U.S. hurricanes*, in International Journal of Disaster Risk Reduction, Vol. 54, 2021, 102043, ISSN 2212-4209.
122 Galluzzo M., (2023), Emergenza e Protezione Civile al tempo dei Social, Palermo, pp..40-41.
123 Lovari A., Murtas F., (2014), Op.cit., p.158.
124 Lombardi M., (2005),Op. cit., pp.94-99.
125 Comunello, Francesca; Mulargia, Simone. Social Media in Earthquake-Related Communication. Emerald Publishing Limited 2018, p.19.
126 Lombardi M., (2005), Op. cit., pp.30-31 e 67-71.

classificate onde evitare che si possano perdere richieste di aiuto magari formulate in modo poco comprensibile. Inoltre per l'utilizzo dell'intelligenza artificiale come sostituto dei soggetti che devono gestire la crisi si pone un problema di assicurazione: come per il caso delle automobili a guida autonoma bisogna chiedersi in caso di malfunzionamento o errore chi paga? Per la circolazione delle *driverless cars* la questione non ha trovato ancora soluzioni pienamente convincenti ed univoche: "da tempo polarizzata sul dilemma etico efficacemente esemplificato mediante la metafora del «*trolley problem*», che scaturisce dalla necessità di programmare *ex ante* decisioni che assumano come soluzione da preferire quella di sacrificare una sola persona o un numero limitato di individui al fine di salvare un numero assai superiore di vite umane. Si tratta, invero, di una questione che non assume rilievo nel sistema attuale, in cui l'esimente dello stato di necessità è ontologicamente riferita a fattispecie nelle quali l'azione astrattamente illecita da cui scaturisce il sacrificio di un diritto è giustificata da situazioni in cui l'individuo si trova costretto ad agire repentinamente al fine di scongiurare pericoli per la vita o l'integrità fisica senza poter programmare ex ante le proprie reazioni istintive. Nel nuovo scenario dominato dalle *driverless cars* l'innovazione tecnologica imporrà di pianificare *ex ante* decisioni tradizionalmente affidate a reazioni impulsive, guidate dall'istinto ed adottate in una dimensione individuale che non postula una valutazione politica da parte del legislatore. Proprio il fatto che le scelte riguardo a situazioni critiche dovrà essere assunto *ex ante*, al momento di programmare le macchine, costituisce, in definitiva, la reale questione posta dall'affermarsi dei veicoli automatici […] Il legislatore, chiamato ad operare nel futuro scenario dominato dall'automazione della circolazione stradale, pertanto, verrà a trovarsi in condizioni non dissimili a quelle che caratterizzano altri contesti in cui si rende necessario effettuare scelte che comportano inevitabilmente l'assunzione di decisioni tese a privilegiare la soluzione funzionale a proteggere il maggior numero di persone, pur nella consapevolezza che essa comporterà necessariamente un sacrificio per un numero sensibilmente inferiore di altri individui che, nondimeno, subiranno danni significativi o fatali "[127]. Un simile ragionamento si può applicare per analogia all'intelligenza artificiale che risponda al posto del responsabile della gestione dell'emergenza, ma con un problema ulteriore da risolvere nel caso in cui il responsabile della gestione sia un soggetto istituzionale: un sindaco e un governatore di regione devono rendere conto del loro operato ai propri cittadini anche in virtù di scelte politiche, mentre, per quanto ben congegnato, l'algoritmo non è democratico, non risponde all'elettorato e non subisce in caso di problemi lo scotto di dimissioni o di una mancata rielezione.

Inoltre l'intelligenza artificiale ha tanta fame di dati per poter essere affidabile nelle risposte e poter raccogliere in maniera adeguata altrettanti dati che possono essere utili: bisogna tenere presente che la maggior parte dei dati di cui si dispone sono forniti dalle piattaforme stesse, i cui algoritmi e criteri di selezione restano segreti[128], senza contare i pregiudizi, che non solo interferiscono nella pratica con l'attività umana di verifica dei fatti, ma creano anche problemi per gli approcci automatici poiché si insinuano nei set di dati che vengono poi utilizzati per addestrare i sistemi di apprendimento automatico, in alcuni casi contribuendo a errori palesi, come ad esempio nel famoso "Gorilla Case"[129]. A questo proposito uno recente e dettagliato studio sul bias cognitivi nel processo di verifica dei fatti –

127 Calabresi G., Al Mureden E., (2020), Driverless car e responsabilità civile, in Rivista di Diritto Bancario, Gennaio/Marzo, 2020, Trento; Al Mureden E., (2024), Diritto dell'automotive, Il Mulino, Bologna.

128 Hand D. J., Dark Data, *Why What You Don't't Know Matters*, Trad. It.: Il tradimento dei numeri, Milano, 2019.

129 Simonite T., (2018), *When it comes to Gorillas, google photos remains blind*. https://www.wired.com/story/when-it-comes-to-gorillas-google-photos-remains-blind/

basato su un elenco completo di 221 bias cognitivi esaminando la letteratura correlata disponibile, da cui è stato estratto un sottoinsieme di 39 pregiudizi che possono manifestarsi durante l'attività di verifica dei fatti – pur arrivando a promuovere un elenco di contromisure per limitarne l'impatto, deve ammettere che per quanto riguarda l'insieme delle contromisure presentate è difficile accertare in che misura le contromisure siano efficaci e generali. La loro efficacia potrebbe essere influenzata da vari fattori, come il contesto specifico, le differenze individuali e la natura della disinformazione"[130].

Il 13 marzo 2024 il Parlamento Europeo ha dato via libera al cosiddetto "*Artificial intelligence act*"[131], un complesso di principi e regolamentazioni che disciplinano uso dell'IA nelle sue innumerevoli applicazioni, distinguendone il livello di rischio tra basso, alto e inaccettabile. Per quanto sopra e in tenendo in particolare considerazione gli scopi della comunicazione d'emergenza, ovvero salvare vite e ridurre la vulnerabilità del sistema, credo che affidare completamente le risposte in comunicazione d'emergenza all'intelligenza artificiale andrebbe inserito nella categoria di rischio più alta dell'*Artificial intelligence act*: inaccettabile. Mentre il rischio sarebbe accettabile nel caso di utilizzo di algoritmi di *clustering* per classificare le domande in entrata, oppure, di *image processing* per verificare l'autenticità delle immagini, oppure l'utilizzo delle tecnologie di *crowdmapping* per una mappatura della crisi in tempo reale. Prima di affidarci totalmente all'intelligenza artificiale anche per la comunicazione d'emergenza, senza fare salti nel futuro, pensiamo ad esempio ai *call center* automatizzati di qualche azienda o di qualche servizio pubblico, che di recente cominciano ad essere implementati attraverso l'intelligenza artificiale: in situazioni di normalità tutti noi abbiamo provato un senso di frustrazione di fronte a risposte rigide e poco afferenti alle nostre richieste e sollecitazioni, ma si pensi all'effetto che potrebbero avere le medesime risposte in situazioni di emergenza, dove magari si rischia la propria vita?

Bibliografia

AGCOM, *Relazione Annuale 2012 sull'attività svolta e sui programmi di lavoro.*

Albanesi E. et al., (2023), Albanesi E., Valastro A., Zaccaria R., *Diritto dell'informazione e della comunicazione*, Wolters Kluwer-Cedam, Milano, 2023.

Al Mureden E., (2024), *Diritto dell'automotive*, Il Mulino, Bologna.

Anzera G., (2014), "*La comunicazione d'emergenza nel conteso contemporaneo*", in Comunello F. (a cura di), (2014), Social Media e Comunicazione d'Emergenza, Milano, pp.21-22.

Anzera G., Massa A., (2021), *Chi ha paura di Internet? Le piattaforme online nei processi di radicalizzazione e di deradicalizzazione*, Franco Angeli, Milano.

Bauman Z. (1999) *In Search of Politics*, Stanford University Press, traduzione italiana: "*La solitudine del cittadino globale*", Feltrinelli, Milano 2000.

Beck U. (1986), *Risikogesellschcaft: Auf dem Weg in eine andere Moderne*, Suhrkamp Verlag, Frankfurt am Main; traduzione inglese del 1992 con il titolo: *Risk Society Towards New Modernity*, SAGE Publications Ltd, California. Successivamente tradotto e pubblicato in italiano da Carocci Editore nel 2000 con il titolo "*La società del rischio. Verso una seconda modernità*."

Beck U. (2007), *Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit*, trad. It.: "*Contitio humana Il rischio nell'età globale*", Mondadori, Milano, 2023.

130 M. Soprano et Al. (2024), Soprano M., Roitero K., La Barbera D., Ceolin D., Spina D., Demartini G., Mizzaro S., Cognitive Biases in Fact-Checking and Their Countermeasures: A Review Information Processing and Management 61 (2024) 103672 February 2024

131 The EU Artificial Intelligence Act: https://artificialintelligenceact.eu/

Bellomo G., (2020), T*rasferimento di dati personali verso paesi terzi: la Corte annulla il «Privacy Shield», amplia i poteri delle autorità di controllo e responsabilizza ulteriormente i data exporters*, in Note e commenti - DPCE on line, 2020/4, online: https://www.dpceonline.it/index.php/dpceonline/article/view/1219
Boccia Artieri G., (2012), *Stati di Connessione. Pubblici, cittadini e consumatori nella (Social) Network Society*, Franco Angeli, Milano.
Bolognini L. et al., (A cura di), (2023), Bolognini L., Pelino E., Scialdone M., (A cura di), (2023), *Digital Services Act e Digital Markets* Act, Giuffrè, Milano
Boyd d., (2010) *Streams of Content, Limited Attention: The Flow of Information through Social Media*, in Web2.0 Expo. New York, NY: November 17, testo disponibile online: https://www.danah.org/papers/talks/Web2Expo.html
Busacca A., (2017), *Il "Diritto di Accesso" alla Rete Internet, Ordine internazionale e diritti umani*, (2017), pp. 345-359, ISSN 2284-3531.
Campagnoli M. N., (2020), *Informazione, Social Network & Diritto*, Key Editore, Milano, 2020.
Calabresi G., Al Mureden E., (2020), *Driverless car e responsabilità civile*, in Rivista di Diritto Bancario, Gennaio/Marzo, 2020, Trento.
Cannaerts N., (2021), *Crisis communication in public emergencies: multistakeholders' perspectives, International Journal of Emergency Services*, 2021, Vol. 10, n.1.
Carrada Giovanni, (2005), *Comunicare la scienza*, Sironi, Milano.
Castells M.,(1996-1998): *The information age. Economy, society and culture:* Volume I, *The rise of the network society* (1996); Volume II, *The power of identity* (1997); Volume III: *End of millennium* (1998). I tre volumi sono stati tradotti in italiano dalla Università Bocconi Editore con i titoli di *La nascita della società in rete* (2002); *Il potere delle identità* (2003); *Volgere di Millennio* (2003).
Colapaoli F. et al., (2021), Colapaoli F., Coppola A., Graziani F.R., Mirone M., ZonaroM., *Social network e diritto*, Giappichelli, Torino, 2021.
Colombo A., (2022), I*l governo mondiale dell'emergenza. Dall'apoteosi della sicurezza all'epidemia dell'insicurezza*, Raffaello Cortina Editore, Milano.
Comunello, Francesca; Mulargia, Simone. Social Media in *Earthquake-Related Communication*. Emerald Publishing Limited 2018.
Coombs W. T., (2020), *Public Sector Crises: Realizations from Covid-19 for Crisis Communication*, reperibile online: http://siba-ese.unisalento.it/index.php/paco/article/view/22498
Coombs W.T., Holladay S.J., (a cura di) (2010), *The Hanbook of Crisis Communication*, Wiley-Blackwell, Chicester.
Coombs, W. T., (2007), *Ongoing Crisis Communication: Planning, Managing, and Responding*, SAGE, Los Angles.
Coombs, W.T. (2014), "*State of crisis communication: evidence and the bleeding edge*", Research Journal of the Institute for Public Relations, Vol. 1 No. 1, pp. 1-12.
Covello et Alii, (2009), Vincent T. Covello, Richard G., Peters J., Wojtecki G., Hyde R. C., *Risk Communication, the West Nile Virus Epidemic, and Bioterrorism: Responding to the Communication Challenges Posed by the Intentional or Unintentional Release of a Pathogen in an Urban Setting*, in Journal of Urban Health, Vol. 78, No. 2, June 2001, pp.382-391, p.386.
Corasaniti G., (2021), *Data science e diritto,* Giappichelli, Torino, 2021.
Dargin et al., (2021), Dargin J., Fan C., Mostafavi A., *Vulnerable populations and social media use in disasters: Uncovering the digital divide in three major U.S. hurricanes*, in International Journal of Disaster Risk Reduction, Vol. 54, 2021, 102043, ISSN 2212-4209.
Dell'Arte S., (2023), *Diritto informazione e comunicazione*, Wolters Kluwer, Milano, 2023.
Delmastro M., Nicita A., *Big data Come stanno cambiando il nostro mondo*, Il Mulino, Bologna, 2019.

Dhoor Singh D., (2024), *Addestramento IA il Garante mette al centro finalità e diritti degli interessati*, in Altalex.it, 14-02-2024: https://www.altalex.com/documents/news/2024/02/13/addestramento-ia-garante-mette-centro-finalita-diritti-interessati.
Farinosi M., Micalizzi A., (a cura di), (2013), *Netquake. Media digitali e disastri naturali*, Franco Angeli, Milano.
Floridi L., (a cura di), (2015), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Springer, New York- London.
Fortunati L. et al., (2018), Fortunati L., Farinosi M., Sarrica M., Ferrin G., Minisini D., Zanut S., *In Caso Di Emergenza. Strategie di comunicazione per la riduzione del rischio a 40 anni dal terremoto del Friuli*, in «Comunicazioni sociali», 2018, n. 2, 246-265, Vita e Pensiero.
Frazer, A.G & Taylor, A.J.W. (1981), *Psychological sequelae of Operation Overdue following the DC10 aircrash in Antartica*, in Psychology, No.27., 72.
Gambino A. M., Mula D., Stazi A., (2021), *Diritto dell'informatica e della comunicazione,* Giappichelli, Torino.
Galluzzo M., (2023), *Emergenza e Protezione Civile al tempo dei Social*, Palermo.
Giddens A. (1990) T*he Consequences of Modernity, Polity Press, Cambridge, traduzione italiana: "Le conseguenze della Modernità"*, Il Mulino, Bologna1994.
Grunig J., (2013), *Excellence in Public Relations and Communication Management, Routledge*.
Hand D. J., Dark Data, *Why What You Don't't Know Matters*, Trad. It.: *Il tradimento dei numeri*, Milano, 2019.
Heil B., Piskorski M., (2009), *New Twitter Research: Men follow men and nobody tweets*, in Harvard Business Review Blog: https://hbr.org/2009/06/new-twitter-research-men-follo
Imperatrice I., (2023), *Tutela dei dati personali sui Social*, in Martorana M., (a cura di), (2023), Diritto e Social Network, Lex Iuris, Bologna, 2023, pp.45-74, p.65.
Jamieson, K., Cappella, J., (2009), *Echo Chamber: Rush Limbaugh and the Conservative Media Establishment*, Oxford University Press; Sunstein, C. R. (2017), #*Republic: Divided Democracy* in The Age of Social Media, Princeton University Press.
Jenkis H., Ford S., Green J., (2013), *Spreadable media: creating value and meaning in a network culture,* NYU Press, New York.
Le Breton D. (1995), *Sociologie du risque*, Presses Universitaires de France, Paris, traduzione italiana Sociologia del rischio, Mimesis Edizioni, Milano, 2017.
Lindsay B. R., (2011) *Social Media and Disasters: Current Uses, Future Options, and Policy Considerations*, report, September 6, 2011; Washington D.C.. (https://digital.library.unt.edu/ark:/67531/metadc93902/: accessed March 26, 2024), University of North Texas Libraries, UNT Digital Library, https://digital.library.unt.edu; crediting UNT Libraries Government Documents Department.
Liu B. F., Austin L., Jin Y., (2011) *How publics respond to crisis communication strategies: The interplay of information form and source,* Public Relations Review, 37(4), 345-353.
Lombardi M., (2005), *Comunicare nell'Emergenza, Vita e Pensiero*, Milano.
Longo E., (2023), *Giustizia digitale e Costituzione. Riflessioni sulla trasformazione tecnica della funzione giurisdizionale*, FrancoAngeli, Milano, 2023.
Lovari A., Murtas F., (2014), *Comunicazione di crisi e pratiche digitali di engaement: il caso della mappa condivisa SardSos"*, in Comunello F. (a cura di), (2014), Social Media e Comunicazione d'Emergenza, Milano.
Luhmann N. (1991), *Soziologie des Risikos, Walter de Gruyter & Co*., Berlin, traduzione italiana: "Sociologia del rischio", Bruno Mondadori 1996
Martorana M., (a cura di), (2023), *Diritto e Social Network, Lex Iuris*, Bologna, 2023.

McConnell B., Huba J., (2010), *The 1% Rule: Charting citizen participation*, La regola dell'1% è stata coniata nel maggio del 2006 dai blogger Ben McConnell e Jackie Huba: The 1% Rule: Charting citizen participation, su churchofthecustomer.com. URL consultato il 16 aprile 2011 (archiviato dall'url originale l'11 maggio 2010).
Mitchell J.T. and Everly G.S. (1997) *Critical Incident Stress Management: a new era and standard of care in crisis intervention,* Ellicott City, MD.: ed.Chevron Publishing Corporation.
Montagnani E., (2021), *La comunicazione pubblica on-line e la digitalizzazione delle Pubbliche amministrazioni tra pandemia e infodemia*, in RID, 1-2021, pp.103-137.
Morelli C., (2024), *Intelligenza Artificiale*, Maggioli Editore, Sanarcangelo di Romagna, 2024.
Muto G., (2023), *La digitalizzazione nell'UE: una sfida costituzionale in Media Laws* – Rivista di Diritto dei Media, 21-02-2023, https://www.medialaws.eu/rivista/la-digitalizzazione-nellue-una-sfida-costituzionale/
Nannipieri L., (2014), *Sulla Dichiarazione dei diritti in Internet, Informatica e Diritto*, XL annata, Vol. XXIII, 2014, n.2, pp.127-138.
Pagano U. (2001), *La comunicazione nelle situazioni di rischio*, in Quaderni di Sociologia 25/2001.
Papacharissi Z., Gibson P. L., (2011), *Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites*, in: Trepte, S., Reinecke, L. (eds) "Privacy Online", Springer, Berlin, Heidelberg, p. 76.
Pariser E., (2011), *The Filter Bubble: What the Internet Is Hiding from You*, Penguin Group, New York.
Petrone L., (2002), *Emergenza in Italia*, in Iacono A. e Troiano M., (a cura di), (2002), *Psicologi dell'emergenza*, Editori Riuniti, Roma.
Quantarelli E.L., (a cura di), (1978), *Disaster: Theory and Research, Sage*, California, 1978.
Rodotà S., (2000), Discorso del prof. Rodotà di presentazione della "*Relazione per l'anno 2000*", reperibile in www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1335256
Schepisi C., (2022), *Diritto fondamentali, principi democratici e rule of law quale ruolo e quale responsabilità per gli Stati nella regolazione dell'intelligenza* Artificiale, in Studi sull'integrazione Europea – SIE, XVII – 2022, pp.41-66.
Simonite T., (2018), *When it comes to Gorillas, google photos remains blind*. https://www.wired.com/story/when-it-comes-to-gorillas-google-photos-remains-blind/
Soprano M. et Al. (2024), Soprano M., Roitero K., La Barbera D., Ceolin D., Spina D., Demartini G., Mizzaro S., Cognitive Biases in *Fact-Checking and Their Countermeasures: A Review Information Processing and Management* 61 (2024) 103672 February 2024
Sturloni G., (2006), *Le mele di Chernobyl sono buone. Mezzo secolo di rischio tecnologico*, Sironi, Milano, 2006.
Sturloni G., (2018), *La comunicazione del rischio per la salute e per l'ambiente*, Mondadori, Milano, pp.5-8.
Van Dijck J., (2013), *Facebook and Engineering of Coonectivity: A multi-layered approach to social media platforms*, in "*Convergence*", vol.19, n. 2.
Talamo S., Di Costanzo F., Crudele R., (a cura di), (2018), *Social Media e PA, dalla formazione ai consigli per l'uso*, Formez PA, 2018.
Van Dijck J., (2013), *The Culture of Connectivity. A Critical History of Social Media*, Oxford University Press, New York.
Van Dijck J., Poell T., (2013), *Understanding Social Media Logic*, in "*Media and Communication*", 2013, Vol.1, n.1, pp. 2-14.
Vittadini N., (2018), *Social Media Studies*, Franco Angeli, Milano.

Yi, C.J. and Kuri, M. (2016), *The prospect of online communication in the event of a disaster, Journal of Risk Research*, Vol. 19 No. 7.
Zarriello R., Cichetti C., (2020), *Comunicazione e Informazione Digitale tra Gestione dell'Emergenza e Ripresa*, Open Comunicazione, 2020.
Ziccardi G., (2022), *Diritti Digitali. Informatica giuridica per le nuove professioni*, Raffaello Cortina Editore, Gravellona Toce (VB), 2022.
Zuccaro A., (2021), *La comunicazione nella gestione delle emergenze*, Palermo.