CYBER ATTACCHI E INCIDENTI NELLA PUBBLICA AMMINISTRAZIONE, FRA ORGANIZZAZIONE AMMINISTRATIVA E CONDOTTA DEL FUNZIONARIO

[ENG] *Cyber attacks and incidents in public administration, between administrative organisation and official conduct*

STEFANO ROSSA
Università degli Studi del Piemonte Orientale
(Italia)
stefano.rossa@uniupo.it

Riassunto: Il contributo analizza il tema della cybersicurezza nel contesto della Pubblica Amministrazione. Dopo aver brevemente ricostruito il concetto di cybersicurezza sul piano giuridico, l'elaborato si interroga se la principale causa di cyber attacchi e incidenti nelle Istituzioni pubbliche dipenda dal modello organizzativo amministrativo adottato oppure dall'azione e dalla condotta dei singoli funzionari. Nelle conclusioni viene invece sottolineata l'importanza della cultura della cybersicurezza, e della centralità dell'alfabetismo digitale, per una corretta gestione del rischio cyber.

Parole chiave: cybersicurezza; cyber-attacchi; cyber-incidenti; organizzazione amministrativa.

Abstract: The paper analyses the topic of cyber security in the context of public administration. After briefly reconstructing the concept of cybersecurity in legal terms, the paper questions whether the main cause of cyber attacks and incidents in public institutions depends on the administrative organisational model adopted or on the actions and conduct of individual officials. Instead, the conclusions emphasise the importance of cyber security culture, and the centrality of digital literacy, for proper cyber risk management.

Keywords: cybersecurity; cyber attacks; cyber incidents; administrative organisation.

1. Introduzione. Il concetto di cybersicurezza e la centralità del momento organizzativo

L'etimologia della parola italiana "cybersicurezza" rivela fin da subito le sue radici straniere, essendo la traduzione del lemma inglese "*cybersecurity*"[1].

Nonostante il confisso "*cyber*" sia di origine greca (*cybernetiké*)[2], la sua attuale accezione *de plano* riconduce al mondo anglofono e al settore tecnologico-digitale. Sebbene una parte della letteratura scientifica, a partire dagli anni Cinquanta, avesse recuperato tale termine attribuendogli un significato diverso dalla sua radice[3], questo collegamento logico è frutto della pubblicazione del famoso romanzo *Neuromante* (orig. *Neuromancer*) di W. Gibson, fondatore del filone letterario cyberpunk, il quale inventò il concetto di "*cyberspace*" per indicare una realtà virtuale alternativa a quella reale e resa possibile grazie alla tecnologia[4].

Il suffisso inglese "*security*", invece, indica "*the things that are done to keep someone or something safe*"[5], vale a dire quell'attività organizzativa volta a ottenere una condizione di sicurezza ("*safety*"[6]). Poiché nella lingua italiana il concetto di sicurezza ricomprende entrambi i significati espressi nei termini inglesi "*security*" e "*safety*"[7], la distinzione della formulazione anglosassone appare cruciale per sottolineare un aspetto fondamentale: l'attività organizzativa si pone come fondamento logico del concetto stesso di cybersicurezza.

---

[1] Le riflessioni del presente elaborato concernono il contesto della cybersicurezza pubblica italiana. Per tale ragione, i riferimenti bibliografici, oltre a quelli internazionali, si soffermano in particolare sulle fonti normative e dottrinali italiane. Ciononostante, fra gli autori della letteratura spagnola che si sono occupati di questo tema è possibile richiamare, *ex multis*, Canals Ametller, D. (dir.), *Ciberseguridad. Un nuevo reto para el Estado y los Gobiernos Locales*, Madrid 2021; Fuertes, M., *Metamorfosis del Estado. Maremoto digital y ciberseguridad*, Madrid 2022; Segura Serrano, A., *El desafío de la Ciberseguridad Global*, Valencia 2023.

[2] Termine impiegato nella tradizione greca antica per indicare l'attività di conduzione di imbarcazioni: cf. Taglia, A. (cur.), Gorgias, Platone, Torino 2014, v. 511.

[3] Si pensi, ad esempio, sul piano internazionale a Wiener, N., *Cybernetics: or Control and Communication in the Animal and the Machine*, New York 1948; nonché a Frosini, V., *Cibernetica, diritto e società*, Milano 1968 e a Losano M.G., *Giuscibernetica. Macchine e modelli cibernetici nel diritto*, Torino 1969.

[4] Cf. Gibson, W., Neuromancer, New York 1984.

[5] Cf. voce «Security», in *Cambridge Learner's Dictionary*, Cambridge 2001, p. 575.

[6] Cf. voce «Safety», in *Cambridge Learner's Dictionary*, Cambridge 2001, p. 563: «when you are safe».

[7] In tal senso si riprendono alcune riflessioni formulate in Rossa, S., *Cybersicurezza e Pubblica Amministrazione*, Napoli 2023, p. 11. Sul tema della cybersecurity si vedano, a titolo esemplificativo e in senso ampio, Salvaggio, S.A., González, N., «The European framework for cybersecurity: strong assets, intricate history», in I*nt. Cybersecur. Law* Rev., n. 4/2023, pp. 137 ss.; AA.VV., *Cybersecurity: Our Digital Anchor. A European Perspective, Publication Office of the European Union 2020*, in https://s.uniupo.it/tw4u8; Van Puyvelde, D., Brantly, A.F., *Cybersecurity: Politics, Governance and Conflict in Cyberspace*, Cambridge 2019; Mitrakas, A., «The emerging EU framework on cybersecurity certification», in *Datenschutz und Datensicherheit* 7 (2018), pp. 411 ss.; Sales, N.A., «Regulating cyber-security», in *Northwestern University Law Review* 4 (2013), pp. 1503 ss.; Hathaway, O. et. al., «The law of Cyber-Attack», in *California Law Review* 100.4 (2012), pp. 817 ss.; Kuehl, D.T., «From Cyberspace to Cyberpower: Defining the Problem», in Kramer, F.D., Starr, S.H., Wentz, L.K. (Eds.), *Cyberpower and national security*, Lincoln 2009; Grady, M.F., Parisi, F. (Eds.), *Law and Economics of Cybersecurity*, Cambridge 2005.

Aspetto che, pur nella difficoltà di delineare una definizione univoca di cybersicurezza[8], che risulti al contempo ampia ma precisa, è messo in evidenza da quanto affermato dall'ENISA, l'Agenzia europea per la cybersicurezza[9]: "*Cybersecurity comprises all activities necessary to protect cyberspace, its users, and impacted persons from cyber threats*"[10]. Pertanto, la *cybersecurity* (di seguito, indistintamente, cybersicurezza) è il mezzo tramite cui giungere alla condizione di *cybersafety*, e in modo più dettagliato può essere definita come il sistema organizzativo finalizzato a proteggere le infrastrutture informatico-digitali di organizzazioni complesse, pubbliche o private, realizzato tramite la predisposizione di misure tecniche idonee volte alla tutela di diritti e libertà fondamentali[11]. Cybersicurezza che, dunque, come sottolineato dalla dottrina, costituisce una vera e propria funzione pubblica[12] strumentale alla protezione sia di diritti fondamentali degli individui sia di valori nazionali (es. sicurezza nazionale).

La centralità del momento organizzativo del concetto di cybersicurezza non deve tuttavia stupire, soprattutto se tale contesto viene calato – come qui si intende – nell'ambito della Pubblica Amministrazione. A ben vedere, infatti, esso si pone esattamente nel solco tracciato dal processo di digitalizzazione pubblico, che richiedere agli attori pubblici coinvolti di agire, e organizzarsi per agire, impiegando gli strumenti digitali nella propria attività istituzionale[13].

Poste tali premesse, in considerazione del crescente numero di cyber attacchi e cyber incidenti che colpiscono tutti i Paesi dell'Unione europea, in particolare l'Italia[14], e che interessano soprattutto

[8] Cf. VEALE, M., BROWN I., «Cybersecurity», in *Internet Policy Review* 9 (2020).

[9] ENISA è l'acronimo di European Union Agency for Network and Information Security. Cf. https://www.enisa.europa.eu/. In argomento MARKOPOULOU, D., PAPAKONSTANTINOU, V., HERT P., «The Nis Directive, Enisa's role and the General Data Protection Regulation», in *Computer Law & Security Review* (2019), pp. 1 ss.; e CAROTTI, B., «Le buone prassi sull'innovazione della cybersicurezza. Il documento dell'Enisa», in *Osservatorio Stato Digitale*, IRPA, 2020; sia consentito altresì il riferimento a ROSSA, S., «Administrative Law Reflections on Cybersecurity, and on Its Institutional Actors, in the European Union and Italy», in *Italian Journal of Public Law* 14.2 (2022), pp. 426 ss., in particolare in relazione all'ACN, l'Agenzia italiana per la Cybersicurezza Nazionale (in relazione alla quale si rimanda a quanto riportato infra).

[10] ENISA, ENISA Overview of Cybersecurity and Related Terminology, 2017, p. 6, in https://s.uniupo.it/elyp6, posto che per cyberspace si intende «the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information».

[11] Riflessioni già espresse in ROSSA, S., *Cybersicurezza e Pubblica Amministrazione*, cit., pp. 12-13.

[12] Così URSI, R., «La sicurezza cibernetica come funzione pubblica», in URSI, R. (cur.), *La sicurezza nel cyberspazio*, Milano 2023, pp. 7 ss.

[13] Cf. art. 2 co. 1 d.lgs. n. 82 del 2005 (c.d. Codice dell'amministrazione digitale): "*Lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione*". In argomento CAVALLO PERIN, R., GALETTA, D.U. (cur.), Il diritto dell'Amministrazione Pubblica digitale, Torino 2020; LALLI, A. (cur.), *L'amministrazione pubblica nell'era digitale*, Torino 2022; TORCHIA, L., Lo Stato digitale. Una introduzione, Bologna 2023; AUBY, J.B., DE MINICO, G., ORSONI, G. (cur.*), L'amministrazione digitale*, Napoli 2023. Sia consentito anche il riferimento a ROSSA S., *Contributo allo studio delle funzioni amministrative digitali*, Milano 2021.

[14] Da ultima è stata colpita la Regione Basilicata, come riporta CANORRO, M., «Attacco ransomware contro i sistemi informatici della Regione Basilicata. ACN invia pool operativo», in *CybersecurityItalia*, 30 gennaio 2024, in

il settore pubblico[15], ci si potrebbe interrogare se ciò dipenda in primo luogo da debolezze organizzative interne alla Pubblica Amministrazione o se, invece, la causa principale sia ascrivibile alla condotta – intenzionale, colposa o meno – dei funzionari pubblici che si trovano, coinvolti in attacchi o in incidenti cyber. Interrogarsi su questo aspetto può risultare utile a indagare più approfonditamente i confini della stessa cybersicurezza.

2. Cyber attacchi e incidenti nella Pubblica Amministrazione: questione di organizzazione amministrativa?

Come è stato sottolineato, la società umana esprime bisogni e interessi, per soddisfare i quali ha predisposto un'apposita struttura burocratica, composta da singoli individui investiti di precise attribuzioni e di compiti, i funzionari, e da strutture complesse organizzate in uffici[16]. Con specifico riferimento alla Pubblica Amministrazione, l'organizzazione amministrativa[17] è pertanto "*l'insieme degli apparati organizzativi attraverso i quali viene svolta la funzione amministrativa*"[18]. Organizzazione amministrativa la quale, come è stato evidenziato, essendo un vero e proprio "*disegno preordinato di uffici, e di relative attribuzioni*"[19], risulta così essere il "*complesso degli uffici quali strumenti predisposti dall'ordinamento per la cura degli interessi generali di una comunità*"[20]. In tal senso, il bisogno da soddisfare corrisponde all'interesse pubblico, il quale viene perseguito tramite

https://s.uniupo.it/0f9rs. Per una panoramica degli attacchi in Italia nel corso del tempo, si veda Redazione ANSA, «Growth in cyber attacks in Italy four times global average», in *ANSA*, 9 November 2023, in https://s.uniupo.it/bh0h3.

[15] In proposito si rimanda ai dati contenuti in CLUSIT, *Rapporto 2023 sulla sicurezza ICT in Italia*, ottobre 2023, in https://clusit.it/rapporto-clusit/.

[16] Così Scoca, F.G., «La pubblica amministrazione come organizzazione», in Mazzarolli, L., Pericu, G., Romano, A., Roversi Monaco, F.A., Scoca, F.G. (cur.), *Diritto amministrativo*, I, Bologna 2005, p. 283.

[17] Essendo un tema di ricerca classico del diritto amministrativo, i riferimenti bibliografici su questo argomento sono numerosi. A titolo non esaustivo: Zanobini, G., *Corso di diritto amministrativo, III, L'organizzazione amministrativa*, Milano 1939; Amorth, A., *Lineamenti della organizzazione amministrativa italiana*, Milano 1950; Giannini, M.S., «Gli elementi degli ordinamenti giuridici», in *Riv. trim dir. pubbl*. (1958); Cimmino, S., *L'organizzazione amministrativa nel suo contesto sociale*, Bologna 1959; Treves G., *L'organizzazione amministrativa*, Roma 1964; Bachelet, V., *Profili giuridici della organizzazione amministrativa. Strutture tradizionali e tendenze nuove*, Milano 1965; Nigro, M., *Studi sulla funzione organizzatrice della pubblica amministrazione*, Milano 1966; Pastori, G., *La burocrazia*, Padova 1967; Berti, G., *La pubblica amministrazione come organizzazione*, Padova 1968; Guarino, G., «Sulla utilizzazione di modelli differenziati nella organizzazione pubblica», in *Scritti di diritto pubblico dell'economia*, Milano 1970; Guarino, G., *L'organizzazione pubblica*, Milano 1977; Berti, G., «La parabola della persona Stato (e dei suoi organi)», in *Quaderni fiorentini* (1982-1983), pp. 1001 ss.; Di Gaspare, G., voce «Organizzazione amministrativa», in *Dig. disc. Pubbl*, Vol. X, Torino 1995, pp. 513 ss. Più recentemente invece Franchini, C., «L'organizzazione», in Cassese, S. (cur.), *Trattato di diritto amministrativo*, I, Milano 2003, pp. 306 ss.; Sciullo, G., *L'organizzazione amministrativa: principi*, Torino 2013; e Cavallo Perin, R., Police, A., Saitta, F. (cur.), *Organizzazione delle pubbliche amministrazioni tra Stato nazionale e integrazione europea*, Firenze 2016. In chiave storica, invece, Melis, G., *Storia dell'Amministrazione italiana*, Bologna 1996; nonché Ruffilli, R., «Problemi dell'organizzazione amministrativa nell'Italia liberale», in *Quaderni storici* 6.18 (1971), pp. 699 ss.

[18] Scoca, F.G., «La pubblica amministrazione come organizzazione», cit., p. 285.

[19] Giannini, M.S., «Gli elementi degli ordinamenti giuridici», cit., p. 237.

[20] Nigro, M., *Studi sulla funzione organizzatrice della pubblica Amministrazione*, cit., p. 116.

l'esercizio di funzioni amministrative, fra cui quella organizzativa, anch'essa avente riflessi sulla tutela delle situazioni giuridiche soggettive.

L'organizzazione amministrativa, pertanto, non deve essere intesa unicamente come un sistema coordinato di persone e di mezzi predisposti dall'ordinamento per raggiungere specifici obiettivi[21], ma anche come un sistema architetturale volto a garantire e tutelare diritti soggettivi e interessi legittimi dei singoli individui[22]. È evidente come questi due aspetti siano legati fra loro, dato che la tutela delle situazioni giuridiche soggettive viene concretamente perseguita (anche) attraverso un'ottima organizzazione amministrativa, individuando in modo preciso il responsabile delle diverse funzioni.

Sul versante che qui interesse, contrariamente a quanto accade nelle imprese private, nel settore pubblico non vi è una figura tipica appositamente individuata *ex ante* – risultando dunque responsabile – per i profili di cybersicurezza. Se nelle società private, in particolare quelle più strutturate, è ormai da anni presente la figura del *Chief Information Security Officer* (CISO)[23], nella Pubblica Amministrazione italiana un ruolo simile *ancora* non c'è, essendo incaricati di tale compito figure operanti nel più ampio contesto del processo di digitalizzazione, come ad esempio il responsabile dei sistemi informativi[24], o il responsabile della conservazione digitale[25], oppure il responsabile della transizione digitale nelle Amministrazioni centrali[26], chiamate a dover predisporre e adottare piani di sicurezza informatica.

Ancora in quanto, in data 25 gennaio 2024, è stato presentato al Consiglio dei Ministri italiano uno schema di disegno di legge in materia di reati informatici e di rafforzamento della cybersicurezza

[21] In tal senso CERULLI IRELLI, V., *Corso di diritto amministrativo*, Torino 1997, p. 71.
[22] Così BACHELET, V., *Profili giuridici della organizzazione amministrativa. Strutture tradizionali e tendenze nuove*, cit., p. 3, il quale ha messo in luce: "*la disciplina giuridica dell'organizzazione della pubblica amministrazione, oltre a stabilirne la struttura con criteri di funzionalità, vuole anche costituire un sistema di garanzia della legittimità e opportunità obiettiva dell'azione e dei procedimenti dell'amministrazione pubblica, sia nei confronti della collettività, sia nei confronti dei singoli cittadini cui questa azione si rivolge*".
[23] Sul CISO si veda, in senso ampio, TARSITANO, P., «CISO: che fa e come si diventa Chief Information Security Officer», in *Cybersecurity360*, 29 settembre 2023, in https://s.uniupo.it/iz25s.
[24] Sul punto cf. SETTE, S., «Responsabile dei Sistemi Informativi nella PA, il grande dimenticato: il problema», in *Agenda Digitale*, 17 giugno 2019, in https://s.uniupo.it/xug2e.
[25] In argomento FICHERA, I.N., «Responsabile della conservazione: una figura da scegliere con attenzione», in *IPSOA Professioni*, 26 febbraio 2020, in https://s.uniupo.it/gy3pz.
[26] Figura prevista dall'art. 17 d.lgs. n. 82 del 2005 (c.d. Codice dell'amministrazione digitale) e, peraltro, a lungo non istituita, come sottolineato dalla Relazione finale della Commissione parlamentare di inchiesta sulla digitalizzazione della Pubblica Amministrazione: cf. CAMERA DEI DEPUTATI, ATTI PARLAMENTARI, XVII LEGISLATURA (Documenti – Disegni di legge e relazioni), Commissione parlamentare d'inchiesta sul livello di digitalizzazione e innovazione delle pubbliche amministrazioni e sugli investimenti complessivi riguardanti il settore delle tecnologie e della comunicazione. Relazione sull'attività svolta, Doc. XII-bis, n. 14, 2017, Cap. 4, in https://s.uniupo.it/yv0r9.

nazionale[27] che, fra le varie proposte di disposizioni, prevede che le maggiori Pubbliche Amministrazioni italiane[28] debbano indicare un soggetto referente per la cybersicurezza[29]. Esso dovrà essere individuato "*in ragione delle qualità professionali possedute*"[30] e dovrà operare in un'apposita struttura adibita, fra le altre, a funzioni di sviluppo di politiche e procedure di *cybersecurity*, all'aggiornamento dei piani di gestione del rischio informatico, alla produzione e all'aggiornamento di documenti di definizione di ruoli e organizzazione di protezione cyber dell'Amministrazione, nonché al monitoraggio e alla valutazione delle minacce cyber alla sicurezza e delle vulnerabilità dei sistemi informativi [31] . Il referente per la cybersicurezza sarà altresì chiamato a svolgere la funzione di punto di contatto unico dell'amministrazione con l'Agenzia per la cybersicurezza nazionale in relazione a quanto previsto dalla disciplina in materia[32].

Questa disposizione è attualmente allo stato di proposta; dunque, fino a che non sarà approvata e trasformata in legge, occorre soffermarsi sulla disciplina normativa oggi in vigore, che non prevede una figura tipica incaricata dei profili di cybersecurity nell'Amministrazione Pubblica.

La ragione di ciò deriva, almeno in parte, dall'architettura istituzionale della cybersicurezza pubblica nell'Unione europea e, di riflesso, nei Paesi membri, incentrata sulla relazione intercorrente fra l'ENISA e le varie Agenzie nazionali per la cybersicurezza[33].

L'ENISA, istituita con Regolamento (CE) n. 2004/460[34], era stata inizialmente plasmata come un'agenzia europea con compiti limitati di natura prevalentemente tecnico-consultiva a favore dei Paesi membri in materia di sicurezza informatica[35], e con durata temporale limitata[36]. Pochi anni dopo il legislatore europeo è intervenuto in materia introducendo nuove discipline (su tutti la c.d. Direttiva

[27] Schema di disegno di legge recante disposizioni in materia di reati informatici e di rafforzamento della cybersicurezza nazionale, 23 gennaio 2024, il cui testo è consultabile in https://s.uniupo.it/k5g26. In ogni caso si rimanda a https://s.uniupo.it/yxkvk.
[28] Nello specifico: le Amministrazioni centrali, le Regioni, le Province Autonome di Trento e Bolzano, i Comuni con una popolazione superiore ai centomila abitanti, i Comuni capoluoghi di Regione, le Società di trasporto pubblico urbano e le Aziende sanitarie locali. Cf. art. 8 co. 1 e art. 13 schema di disegno di legge recante disposizioni in materia di reati informatici e di rafforzamento della cybersicurezza nazionale, 23 gennaio 2024.
[29] Cf. art. 13 schema di disegno di legge recante disposizioni in materia di reati informatici e di rafforzamento della cybersicurezza nazionale, 23 gennaio 2024.
[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] In argomento, in senso lato, BEDERNA, Z., RAJNAI, Z., «Analysis of the cybersecurity ecosystem in the European Union», in *Int. Cybersec. Law Rew*. 3 (2022), pp. 35 ss., oltre a ROSSA, S., «Administrative Law Reflections on Cybersecurity, and on Its Institutional Actors, in the European Union and Italy», cit.
[34] Regolamento (CE) 2004/460 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.
[35] Cf. artt. 2 e 3 Regolamento (CE) 2004/460.
[36] Cf. art. 27 Regolamento (CE) 2004/460.

NIS[37] e il c.d. *Cybersecurity Act*[38], oltre alla più recente Strategia dell'Unione europea per la cybersicurezza del 2020[39]) e modificando l'impianto originario dell'ENISA[40], con l'esplicito intento di incrementare il livello di resilienza del sistema europeo di cybersicurezza. In particolare, a seguito dell'approvazione del *Cybersecurity Act*, all'ENISA è stato assegnato un ruolo di perno rotante della politica europea di cybersicurezza, divenendo il soggetto istituzionale di riferimento per l'Unione stessa, i Paesi membri, i cittadini e il settore privato[41], come risulta dalle funzioni attribuitele[42]. Innanzitutto, all'ENISA spetta la funzione di assistenza alle Istituzioni, agli organi e agli organismi dell'Unione, nonché a Stati membri, nell'elaborazione e nell'attuazione delle politiche europee di *cybersecurity*, anche tramite azioni di supporto tecnico[43]. In secondo luogo, l'Agenzia è incaricata della funzione di cooperazione operativa, del coordinamento e della condivisione di informazioni di cybersicurezza a livello europeo sia tra gli Stati membri, le Istituzioni, gli organi e gli organismi dell'Unione e i portatori di interessi del settore pubblico e privato; sia fra Unione europea, Paesi terzi e organizzazioni internazionali[44]. A tali compiti si affianca quello mirato a sviluppare le competenze e conoscenze nel campo della cybersecurity[45]. Infine, all'Agenzia spetta altresì la funzione di promozione e di sviluppo della politica unionale in materia di certificazione della sicurezza cibernetica dei prodotti e servizi tecnologici[46].

Dai compiti istituzionali attribuiti all'ENISA emerge come alle tradizionali funzioni tecnico-consultive ne siano state affiancate altre di carattere maggiormente operativo[47]. Ciononostante, la funzione principale di questa agenzia risulta essere quella di "promozione attiva" della *cybersecurity* in tutta l'Unione[48], con l'intento di raggiungere una disciplina di cybersicurezza comune e omogenea

[37] Direttiva 2016/1148/UE Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
[38] Regolamento (EU) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).
[39] Comunicazione della Commissione JOIN (2020) 18 final 16 dicembre 2020. Sul punto KOHLER, C., «The EU Cybersecurity Act and the European Standards. An Introduction to the Role of European Standardization», in *Int. Cybersec. Law Rew*. 1 (2020), pp. 7 ss.
[40] Cf. *ex multis* il Regolamento (CE) 2008/1007, il Regolamento (UE) 580/2011 e il Regolamento (UE) 526/2013.
[41] In proposito si veda il documento di ENISA, *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, 2018, p. 1, in https://s.uniupo.it/qmi9e.
[42] Si consideri che ex art. 68 Regolamento (EU) 2019/881 è venuta meno la durata temporalmente limitata dell'ENISA.
[43] Cf. artt. 4 e 5 Regolamento (EU) 2019/881.
[44] Cf. artt. 4, 7, 9 e 12 Regolamento (EU) 2019/881.
[45] Cf. artt. 4 e 6 Regolamento (EU) 2019/881.
[46] Cf. artt. 4, 8, 10 e 11 Regolamento (EU) 2019/881.
[47] Di tale parere anche CAMPARA, F., «Il Cybersecurity Act», in CONTALDO, A., MULA, D. (cur.), *Cybersecurity Law*, Pisa 2020, p. 72 e BRIGHI, R., CHIARA, P.G., «La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea», in *federalismi.it* 21 (2021), p. 24.
[48] Come si è avuto modo di sottolineare anche in ROSSA, S., *Cybersicurezza e Pubblica Amministrazione*, cit., p. 101.

in tutti gli Stati membri[49]. Aspetto peraltro confermato dall'essere, come anticipato, il perno rotante del sistema istituzionale della cybersicurezza, intorno al quale gravitano in particolare le agenzie nazionali dei vari Paesi membri, in una dimensione che può essere descritta con un modello reticolare decentralizzato a stella[50]. In questa struttura reticolare[51] vi è un nodo centrale che permette il coordinamento del reticolo e permette agli altri nodi, a cui spettano funzioni diverse rispetto al nodo centrale, di entrare in connessione fra loro. In tale modello l'ENISA corrisponderebbe al nodo centrale, mentre le diverse Agenzie nazionali di cybersicurezza dei Paesi membri agli altri nodi. Se all'ENISA spetta la funzione di promozione e coordinamento attivo, alle Agenzia nazionali invece sono attribuiti i compiti operativi nel campo della cybersicurezza, essendo chiamate a dare attuazione alle strategie europee dell'ENISA, uniformando così la disciplina in materia in tutti gli Stati membri.

Come noto, l'attuale *corpus* normativo europeo in materia di cybersicurezza pubblica è costituito dalla Direttiva (UE) 2022/2555[52] (c.d. Direttiva NIS 2), che ha abrogato la Direttiva 2016/1148/UE[53] (c.d. NIS), sul cui impianto tuttavia si innesta, implementandolo[54]. Ed è proprio sulla base di quest'ultimo che ogni Stato membro ha dovuto istituire la propria Agenzia nazionale di *cybersecurity*[55]: l'Italia ha adempiuto a tale obbligo dando vita all'Agenzia per la Cybersicurezza Nazionale (ACN), l'Autorità nazionale italiana competente in materia, all'interno della quale è altresì istituito il *Computer Security Incident Response Team* (CSIRT) italiano[56]. I poteri di cui l'ACN è

[49] Obiettivo che permea tutta la politica europea del digitale, come sottolineato da CAROTTI B., «La politica europea sul digitale: ancora molto rumore», in *Riv. trim. dir. pubbl.* 4 (2022), pp. 997 ss.
[50] Considerazioni già evidenziate in ROSSA, S., «Administrative Law Reflections on Cybersecurity, and on Its Institutional Actors, in the European Union and Italy», cit., pp. 445 ss.
[51] Modello elaborato da BARABÀSI, A.L., Linked. The New Science of Networks, Cambridge 2002, pp. 143 ss.
[52] Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2). La Direttiva NIS 2 è entrata in vigore nel gennaio 2023 e gli Stati membri sono tenuti recepirla entro l'ottobre 2024. Conseguentemente la disciplina attualmente in vigore è quella nazionale di recepimento della Direttiva NIS, per l'Italia il d.lgs. n. 65 del 2018.
[53] Vedasi la nota 37.
[54] Non si ritiene necessario approfondire in questa sede l'analisi della disciplina dettata dalla Direttiva NIS 2, e della sua differenza rispetto a quella della Direttiva NIS. Si rimanda, pertanto, a KAISER, E., «The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations», in *Media Laws – Rivista di Diritto dei media* 1 (2023), pp. 343 ss.; PALLADINO, A., «Cybersecurity: adottata la Direttiva NIS2 per rafforzare la resilienza», in *Osservatorio sullo Stato Digitale*, IRPA, marzo 2023; BAVETTA, F., «Direttiva NIS 2: verso un innalzamento dei livelli di cybersicurezza a livello europeo», in *Media Laws – Rivista di Diritto dei media* 3 (2022), pp. 405 ss.
[55] Cf. artt. 7 e 8 alla Direttiva 2016/1148/UE.
[56] L'ACN è stata istituita con decreto-legge n. 82 del 2021, convertito con modificazioni in legge n. 109 del 2021. Il suo sito web istituzionale è https://www.acn.gov.it/. In argomento si vedano CUSENZA, G.G., «I poteri dell'Agenzia per la Cybersicurezza Nazionale: una nuova regolazione del mercato cibernetico», in URSI, R. (cur.), *La sicurezza nel cyberspazio*, cit., pp. 123 ss.; SERINI, F., «La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021», in *federalismi.it* 12 (2022), pp. 241 ss.; FORGIONE, I., «Il ruolo strategico dell'Agenzia Nazionale per la Cybersecurity nel contesto del sistema di sicurezza nazionale: organizzazione e funzione, fra regolazione europea e interna», in *Dir. amm.* 4 (2022), pp. 113 ss.; PARONA, L., «L'istituzione dell'Agenzia per la cybersicurezza nazionale», in *Giorn. dir. amm.* 6 (2021), pp. 709 ss.; sia consentito il rimando a ROSSA, S., *Cybersicurezza e Pubblica Amministrazione*, cit., pp. 65 ss.

dotata – funzioni principalmente[57] ascrivibili al coordinamento dei soggetti operanti sul territorio nazionale nell'ambito della cybersicurezza; alla promozione e alla realizzazione di piani di cybersicurezza (tra cui la Strategia nazionale di Cybersicurezza[58]); all'attività consultiva in materia di *cybersecurity* a favore di Governo e Parlamento; alla certificazione di cybersicurezza; nonché alla vigilanza e sanzione (in precise ipotesi) – così come l'attuale disciplina nazionale in materia di *cybersecurity*, non hanno imposto l'adozione di un una figura tipica responsabile dei profili di cybersicurezza. E questo in forza del principio di auto-organizzazione amministrativa[59] che, nell'ipotesi di mancanza di espresse previsioni normative, consente alle singole amministrazioni di dotarsi discrezionalmente della struttura organizzativa ritenuta più adeguata al raggiungimento dei fini posti dalla disciplina europea e nazionale – fra cui rientra proprio l'adozione di misure organizzative per gestire correttamente attacchi e incidenti cyber[60].

L'assenza di una figura tipica responsabile della cybersicurezza nella Pubblica Amministrazione non consente di poter attribuite automaticamente all'aspetto organizzativo la causa principale degli attacchi e degli incidenti cyber che interessano i soggetti pubblici. Anzi, a ben vedere, la presenza di molteplici figure responsabili dei profili di *cybersecurity*, pur essendo atipiche, testimonia gli sforzi organizzativi compiuti dalle Amministrazioni nell'adattare la propria struttura alle nuove esigenze di sicurezza informatica.

Al limite, tale atipicità potrebbe condurre a interrogarsi su quali competenze abbiano effettivamente i soggetti chiamati a ricoprire tale ruolo nelle Pubbliche Amministrazioni, e dunque a interrogarsi sul profilo della condotta dei funzionari.

3. Cyber attacchi e incidenti nella Pubblica Amministrazione: questione di condotta del funzionario?

Fino a qui si è fatto riferimento, in senso ampio, al concetto di cybersicurezza. In realtà, come è stato sottolineato[61], tale concetto racchiude in sé alcune sottocategorie che possono essere considerate

[57] In ogni caso cf. art. 7 d.l. n. 82 del 2021, conv. l. n. 109 del 2021.
[58] Cf. ACN, *Strategia nazionale di cybersicurezza 2022-2026*, in https://s.uniupo.it/tcl0n.
[59] Si consideri che, nell'ambito del public procurement, questo principio è stato inserito fra quelli fondamentali sui quali si basa la disciplina del nuovo codice dei contratti pubblici italiani: cf. art. 7 d.lgs. n. 36 del 2023. In senso ampio, sul principio di autorganizzazione come espressione di sussidiarietà si veda Perfetti, L.R., «L'organizzazione amministrativa come espressione della sovranità», in *Dir. Econ*. 1 (2019), pp. 61 ss.
[60] Cf. *ex multis* art. 24 co. 2 Direttiva (UE) 2022/2555.
[61] In tal senso l'importante documento della Presidenza del Consiglio dei Ministri, *Quadro Strategico annuale per la sicurezza nello spazio cibernetico*, Roma 2013, pp. 12-13, in https://s.uniupo.it/tpa5s.

sue componenti costitutive, riflettendo la natura delle diverse minacce cyber che in essa possono verificarsi[62]: *cyber-intelligence*, *cyber-warfare*, *cyber-crime*, *cyber-terrorism* e cyber-resilienza[63].

In Italia, esse corrispondono a specifiche aree di intervento la cui competenza è affidata a distinti soggetti: la *cyber-intelligence* al Dipartimento delle informazioni per la sicurezza (DIS)[64], il *cyber-crime* e il *cyber-terrorism* al Ministero dell'Interno, specificamente alla Polizia Postale e delle Comunicazioni[65], il *cyber-warfare* al Ministero della Difesa, in particolare al Reparto Sicurezza Cibernetica (RSC)[66], mentre la cyber-resilienza all'Agenzia per la Cybersicurezza Nazionale (ACN).

Questa circostanza pone in luce un dato chiaro: l'alta attenzione delle Istituzioni pubbliche ai temi della cybersicurezza, in conseguenza della sua rilevanza in una pluralità di contesti considerati storicamente sensibili per gli interessi pubblici, ma oggi ancora di più a seguito della pervasività delle tecnologie digitali[67]. Attenzione che si è tradotta nella creazione di apposite Amministrazioni dotate di personale altamente qualificato.

---

[62] Sul punto anche MATTARELLA, A., «Gli aspetti penali del cybercrime: la Convenzione ONU sulla criminalità informatica», in URSI, R. (cur.), *La sicurezza nel cyberspazio*, cit., p. 202.

[63] Quest'ultima non ricompresa nell'elencazione effettuata in PRESIDENZA DEL CONSIGLIO DEI MINISTRI, *Quadro Strategico annuale per la sicurezza nello spazio cibernetico*, cit., ma divenuta effettiva con l'istituzione dell'Agenzia per la Cybersicurezza Nazionale.

[64] Il DIS rientra nel Sistema di informazioni per la Sicurezza della Repubblica (SISR), i servizi segreti italiani. Cf. https://s.uniupo.it/v8c26. In argomento RIDOLFI, M., «Servizi di informazione e cybersicurezza», in *Giornale di diritto amministrativo* 2 (2023), pp. 207 ss.; TETI, A., *Cyber espionage e cyber counterintelligence. Spionaggio e controspionaggio cibernetico*, Soveria Mannelli 2018.

[65] Cf. https://s.uniupo.it/tgews. In tema di cyber-crime si vedano RIZZUTO, R., «Cybercrime e la svolta digitale della giustizia penale: approdi e possibili scenari», in *Archivio della nuova procedura penale* 1 (2023), pp. 29 ss. e MATTARELLA, A., «Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite», in *Diritto penale e processo* 6 (2022), pp. 809 ss. Per quanto invece attiene al cyber-terrorism si veda MELE, S., «Cyberterrorismo e radicalizzazione online», in ZICCARDI, G., PERRI, P. (cur.), *Tecnologia e diritto, III, Informatica Giuridica Avanzata*, Milano 2019, pp. 313 ss.

[66] Sul punto MARRONE, P., «Eternal Hobbes: International Relations and Cyberwar», in *Etica & politica* 1 (2023), pp. 449 ss.; WHYTE C., MAZANEC, B.M., *Understanding Cyber Warfare: Politics, Policy and Strategy*, Londra 2019; KAPLAN, F., *Dark Territory: The Secret History of Cyber War*, New York 2016; TSAGOURIAS, N., BUCHAN, R. (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham 2015; MAOGOTO, J., *Technology and the Law on the Use of Force: New Security Challenges in the Twenty-First Century*, Londra 2014; LIBICKI, M.L., *Conquest in Cyberspace. National Security and Information Warefare*, Cambridge, 2007. Tra le fonti giornalistiche si rimanda a BUSSOLETTI, F., «Cyber Warfare, anche l'Italia ha le sue "forze speciali" cyber», in *Difesa e sicurezza* (2021), in https://s.uniupo.it/1zz5b; nonché il recente articolo di DI FEO, G., «L'esercito italiano cambia pelle: due nuovi reggimenti per gestire droni e combattimenti cyber», in *La Repubblica*, 24 gennaio 2024, in https://s.uniupo.it/f00g9.

[67] Si pensi, ad esempio, alla crittografia. Già dai tempi degli antichi romani era sorta la necessità di proteggere le comunicazioni militari tramite sistemi di crittografia, come testimoniato da Svetonio nella sua opera De vita Caesarum, I, 56, in relazione al c.d. cifrario di Cesare. Cf. MARCHESI, C. (cur.), *Svetonio. Vite dei Cesari. Volgarizzate da Giuseppe Rigutini*, Firenze 1946, pp. 36-37, che riporta: *"[r]imangono pure alcune lettere a Cicerone, come anche ai suoi familiari sopra a cose domestiche. Quando non voleva essere inteso dagli altri, scriveva in cifra, cioè confondendo l'ordine alfabetico delle lettere, per modo che era impossibile comporne alcuna parola. Chi voglia decifrarle, preda la lettera d in luogo dell'a, e così di seguito*". In relazione al rapporto fra sicurezza delle comunicazioni militari e fattore umano, si rimanda alle interessanti considerazioni di KERCKHOFFS, A., «La cryptographie militaire», in *Journal des sciences militaires* 9 Gen. (1883), pp. 5 ss. e Febr. 1883, pp. 161 ss. È chiaro che la tecnologia digitale ha potenziato tanto la l'attività di criptazione quanto quella di decriptazione, ma aumentando in modo esponenziale la disponibilità di strumenti in grado di compiere queste operazioni.

Tuttavia, proprio la pervasività della digitalizzazione in ogni settore e in ogni ambito dimensionale potrebbe indurre a chiedersi se l'istituzione tali Amministrazioni *ad hoc* sia sufficiente, dal momento che tutte le Pubbliche Amministrazioni, anche quelle più piccole e periferiche, sono esposte a rischi di cybersicurezza, dovendo anch'esse esercitare funzioni amministrative, e prestare servizi pubblici, tramite le ICT.

Posto che in Italia vi sono circa tredicimila Amministrazioni, di cui circa ottomila sono Comuni[68] – dei quali il meno denso abitativamente è Morterone (LC) con trentuno abitanti[69] – risulta dunque evidente l'eterogeneità di condizioni fra le (poche) Amministrazioni preparate sul versante cyber e le (molte) altre Amministrazioni di medie e piccole-piccolissime dimensioni, sovente dotate di una pianta organica limitata a cui spettano compiti molto diversificati. Al di là dell'esternalizzazione dell'attività di *cybersecurity*, è evidente che queste circostanze incidano sull'azione e sulla condotta dei funzionari, i quali spesso non possiedono le necessarie competenze digitali che, se invece possedute, potrebbero evitare il verificarsi – non intenzionale, sia chiaro, ma al limite colposo[70] – di cyber attacchi e cyber incidenti. Emblematico a tal proposito è quanto accaduto nel 2021 a Roma, in occasione di un attacco informatico (di tipo *ransomware*, cui *infra*) che ha colpito la Regione Lazio per il tramite di un computer di un dipendente che lavorava da remoto[71]. Questo fatto sorprende soltanto parzialmente, purtroppo, se si analizza la *Relazione annuale al Parlamento* del 2022 dell'Agenzia per la Cybersicurezza Nazionale, dalla quale emerge che il *ransomware* sia lo strumento più impiegato dagli attaccanti per arrecare cyber attacchi nella Pubblica Amministrazione, specialmente nei Comuni e nelle Regioni[72], mentre gli attacchi DDoS (*Distributed Denial of Service*), che causano un malfunzionamento al bersaglio "intasando" le risorse del sistema informatico, sono prevalentemente indirizzati verso Amministrazioni centrali e Organi a rilevanza costituzionale (Amministrazioni dotate di personale specializzato anche in ambito digitale).[73] Come noto, infatti, i

[68] Cf. ISTAT, *Censimento permanente delle Istituzioni pubbliche: registri e rilevazione censuaria multiscopo*, Roma, Roma, 2023, 37, in https://s.uniupo.it/089ll, in cui sono riportate le cifre precise: 13.038 Pubbliche Amministrazioni, di cui 7.903 Comuni.
[69] Cf. la banca dati ISTAT con dati del 2023 all'indirizzo https://s.uniupo.it/osent.
[70] Posto che, come noto, secondo l'art. 43 del Codice penale italiano la colpa può essere specifica (nel caso di inosservanza di leggi, regolamenti, ordini e discipline) o colpa generica, quest'ultima nell'ipotesi di negligenza, imprudenza o imperizia.
[71] In tal senso NAVACCI, M., «Regione Lazio e ransomware, lieto fine amaro: troppi errori fatti», in *Cybersecurity360* 8 agosto (2021), in https://s.uniupo.it/dl1rf, che ricostruisce la vince e riporta: "*[a]l momento la versione ufficiale è che il dipendente […] sia stato contagiato da malware (forse per aver cliccato su un link in mail phishing; forse può averlo fatto il figlio che ha usato il computer del padre di notte)*".
[72] ACN, *Relazione annuale al Parlamento*, Roma 2022, pp. 50-51, in https://s.uniupo.it/19ziv.
[73] Ibid. In argomento DENNIS, M.A., voce «Denial of Service Attack», in *Encyclopaedia Britannica* (2023), in https://s.uniupo.it/q91l2.

ransomware sono *malware*[74] che infettano un dispositivo impedendone l'accesso, o bloccando il dispositivo (i c.d. *r. blocker*) o criptandone i dati (i c.d. *r. cryptor*), e richiedendone successivamente il riscatto (in inglese "*ransom*")[75]: essi si diffondono prevalentemente attraverso il *download* di file allegati a messaggi e-mail malevoli o cliccando su link malevoli[76]. È dunque necessario – quasi sempre[77] – un comportamento attivo del soggetto bersaglio, il quale agisce senza intenzione né consapevolezza dei rischi che sta correndo, ma la sua (pur inconsapevole) condotta comporta ingenti danni all'Amministrazione se questi è un funzionario pubblico. Questa circostanza è il riflesso di una sorta di "proporzionalità" di cyber-attacco degli attaccanti: esattamente come tale principio impone che "*la polizia non deve sparare ai passeri con i cannoni*"[78], gli attaccanti usano strumenti più semplici (*ransomware*) quando devono colpire bersagli "semplici" (le Amministrazioni più piccole e periferiche), mentre ricorrono a strumenti più sofisticati e complessi (DDoS) quando devono colpire Amministrazioni maggiormente consapevoli dei rischi.

Il fattore umano è dunque centrale nella cybersicurezza, sia nel settore pubblico sia in quello privato[79]: il tema della condotta del funzionario risulta essere, pertanto, una delle più importanti cause di cyber attacchi e incidenti. Ma questo tema, in realtà, ne nasconde e ne sottointende la causa: esso dipende e deriva fortemente dal grado di cultura e di alfabetizzazione digitale delle persone, siano esse funzionari pubblici o meno.

4. Conclusioni: la centralità dell'alfabetizzazione digitale e della cultura della cybersicurezza

Come noto, ogni anno la Commissione europea pubblica il DESI (*Digital Economy and Society Index*), un indice molto articolato che illustra i progressi che l'Unione europea e gli Stati membri hanno compiuto in materia di digitalizzazione rispetto all'anno precedente[80]. Uno fra gli indicatori

[74] In proposito di rimanda alle riflessioni di Dal Checco, P., *La protezione dal malware*, in Ziccardi, G., Perri, P. (cur.), *Tecnologia e diritto*, III, *Informatica Giuridica Avanzata*, Milano 2019, pp. 225 ss.
[75] Cf. Volle, A., voce «Ransomware», in *Encyclopaedia Britannica* (2024), https://s.uniupo.it/97n9m. Sul punto anche Richardson, R., North, M.N., «Ransomware: evolution, mitigation and prevention», in *International Management Review* 1.13 (2017), pp. 10 ss.
[76] Come è sottolineato dalla scheda tematica predisposta dal Garante per la Protezione dei Dati Personali, *Ransomware*, in https://s.uniupo.it/22ply, è altresì possibile, seppur meno frequente, che i ransomware siano installati tramite malware di controllo remoto del dispositivo.
[77] Ibid.
[78] Questa la nota figura retorica elaborata da Fleiner, F., *Institutionen des Deutschen Verwaltungsrechts*, Tübingen 1911, p. 345.
[79] Cf. Castigli, M., «Sicurezza informatica nelle Pmi: a causare i danni sono spesso i dipendenti», in *Cybersecurity360*, 9 giugno 2023, in https://s.uniupo.it/5xlp7.
[80] L'indice è consultabile sul sito istituzionale della Commissione europea all'indirizzo https://s.uniupo.it/z3i5c.

del DESI 2022 fotografa il "Capitale umano", vale a dire il grado di conoscenza e di utilizzo delle tecnologie dei cittadini, analizzando in particolare la percentuale di individui in possesso di competenze digitali di base, di quelle superiori alla media, e di quelle di base necessarie a creare contenuti digitali; ma esamina altresì la percentuale di laureati in discipline informatico-digitali (ICT), quella degli specialisti ICT (e di quanti di essi sono di sesso femminile), nonché la percentuale di imprese che forniscono formazione in materia ICT[81]. A livello di Unione europea, poco più della metà degli individui (54%) possiede competenze digitali basiche, ma soltanto un quarto (26%) dimostra competenze digitali superiori. Nell'Unione soltanto una persona ogni venticinque si laurea in materie ICT (3,9%), aspetto che riflette il mercato del lavoro, nel quale soltanto un lavoratore su ventidue è specialista ICT (4,5%)[82]. Più interessante è analizzare, invece, questo indice a seconda dei Paesi membri. Se sul podio si collocano Finlandia (1° su 28), Paesi Bassi (2°) e Irlanda (3°), l'Italia si inserisce nella parte bassa della classifica (25°), prima di Portogallo (26°), Bulgaria (27°) e Romania (28°)[83]. Mentre in Finlandia quasi quattro persone su cinque possiedono conoscenze digitali basiche (79%) e uno su due (48%) conoscenze digitali avanzate[84], nel Bel Paese poco meno di un italiano su due ha conoscenza digitali basiche (46%) e meno di uno su quattro (23%) conoscenze ICT avanzate[85]. Proprio il "Capitale umano" è l'indicatore del DESI nel quale l'Italia si colloca più in basso nella classifica degli Stati membri (25° posizione), mentre in "Connettività" (7°) e "Integrazione delle tecnologie digitali" (8°) è abbondantemente sopra la media europea, mentre in "Servizi pubblici digitali" (19°) poco sotto[86].

Il livello di analfabetismo digitale degli italiani è dunque molto elevato. E ciò è la conseguenza di concause[87] di natura sociale – come l'età media della popolazione elevata (46,4 anni)[88] –, educative – fra cui la bassa percentuale di studenti laureati nella fascia 30-34 anni (26,8% rispetto al 41,6% della media UE)[89] e, in generale, di numero di laureati nella società (solo il 14% possiede una

[81] Cf. EUROPEAN COMMISSION, *Digital Economy and Society Index 2022 – Thematic Chapters*, 2023, pp. 20 ss., in https://s.uniupo.it/v9us8.
[82] Ibid.
[83] EUROPEAN COMMISSION, *Digital Economy and Society Index 2022 – Thematic Chapters*, cit., p. 24.
[84] Cf. EUROPEAN COMMISSION, *DESI 2022 Country Profile: Finland*, 2023, p. 6, in https://s.uniupo.it/w0r4a.
[85] Cf. EUROPEAN COMMISSION, *DESI 2022 Country Profile: Italy*, 2023, p. 7, in https://s.uniupo.it/5jahn.
[86] Nella classifica complessiva del DESI 2022, considerato in tutti i suoi indicatori componenti, l'Italia si colloca al diciottesimo posto su ventotto Paesi. Cf. EUROPEAN COMMISSION, *DESI 2022 Country Profile: Italy*, cit., pp. 4-5.
[87] In tal senso anche ISTITUTO NAZIONALE DI STATISTICA (ISTAT), *Società: Cittadini e competenze digitali*, 22 giugno 2023, pp. 3 ss., in https://s.uniupo.it/v30m0.
[88] Cf. ISTITUTO NAZIONALE DI STATISTICA (ISTAT), *Rapporto annuale 2023. La situazione del Paese*, Roma 2023, p. 37, in https://s.uniupo.it/u9xn6, dal quale emerge altresì che il 24,1% della popolazione italiana ha più di sessantacinque anni, mentre soltanto il 12,5% ha meno di quattordici anni.
[89] Cf. ISTITUTO NAZIONALE DI STATISTICA (ISTAT), *Report: Livelli di istruzione e ritorni occupazioni*, Anno 2021, 25 ottobre 2022, 1 ss., in https://s.uniupo.it/o7shn.

istruzione universitaria)[90] – e informatiche – fra cui la carenza di infrastrutture digitali in determinate aree geografiche del Paese, in particolare nel Sud Italia e nelle aree interne e montane, che comportano un vero e proprio *digital divide*[91].

Come è stato rilevato dall'Eurostat, il livello di analfabetismo digitale è proporzionale all'aumentare dell'età anagrafica degli individui[92], nell'Unione europea e nei Paesi membri. In Italia, questo dato si ripercuote inevitabilmente nella stessa Pubblica Amministrazione, caratterizzata da un'età media dei dipendenti superiore a 50 anni, cresciuta significativamente negli anni[93], e in cui i funzionari appartenenti alla c.d. generazione dei "nativi digitali" sono ancora molto pochi (solo il 4,2% ha meno di trent'anni)[94].

L'alto tasso di analfabetismo digitale si traduce (*inter alia*) in un uso poco consapevole dei dispositivi digitali, portando a sottovalutare rischi e pericoli intrinsecamente presenti nel web. È evidente che un simile comportamento, posto in essere in un contesto lavorativo, può tradursi in condotte dannose sia per il dipendente sia per lo stesso datore di lavoro, che può vedere compromessa l'integrità dei propri sistemi informativi. Ed è altrettanto chiaro che tale situazione ha effetti ancora più dirompenti qualora ciò dovesse accadere – come sovente accade – nella Pubblica Amministrazione[95].

In questo senso, la mancanza di un maturo alfabetismo digitale e di una cultura digitale diffusa, in particolare di quella della cybersicurezza, costituisce la principale causa degli attacchi e degli incidenti che si verificano nelle Amministrazioni Pubbliche italiane, rappresentando un fattore centrale nelle condotte individuali dei funzionari, unitamente alla menzionata (non ancora funzionale) condizione organizzativa amministrativa del digitale – su cui per l'appunto è intervenuto lo schema

[90] Cf. DA ROLD, C., «Perché in Italia i 30-34enni con una laurea sono solo il 26,8%?», in *Il Sole 24 Ore*, Info Data: Le notizie raccontate con i numeri, 31 luglio 2023, in https://s.uniupo.it/576ti.
[91] In argomento REDAZIONE FORUM PA, «Digital divide, l'accesso a internet al Sud non per tutti. Il ruolo degli operatori di mercato», in *Forum PA*, 25 luglio 2023, in https://s.uniupo.it/dio6y. Per un'analisi dettagliata della situazione nelle varie Regioni italiane, in relazione ai dati del 2020, si veda il report di OPEN POLIS, *Disuguaglianze digitali*, 2020, in https://s.uniupo.it/cisvh.
[92] Cf. EUROSTAT, Community survey on ICT usage in Households and by Individual, citato in EUROPEAN COMMISSION, *Digital Economy and Society Index 2022 – Thematic Chapters*, cit., p. 24: il 71% degli individui europei fra 16 e 24 anni possiedono almeno competenze digitali basiche, mentre queste ultime sono possedute dal 69% degli individui fra 25 e 34 anni, dal 64% di quelli fra 35 e 44, del 55% di quelli fra 45 e 54 anni, del 42% di quelli fra 55 e 64 e del 25% di quelli fra 65 e 74 anni.
[93] Si veda il documento sviluppato dal MINISTERO DELL'ECONOMIA E DELLE FINANZE – DIPARTIMENTO DELLA RAGIONERIA GENERALE DELLO STATO, *Distribuzione dei dipendenti per età, 2021*, in https://s.uniupo.it/lhncp. In argomento anche BELLA, E., «L'occupazione nel settore pubblico in Italia», in *Osservatorio Conti Pubblici Italiani – Università Cattolica del Sacro Cuore*, 2022, in https://s.uniupo.it/gdjqq.
[94] Cf. MINISTERO PER LA PUBBLICA AMMINISTRAZIONE, Pa, necessarie più di 700.000 assunzioni entro il 2025, 2021, in https://s.uniupo.it/djr2a.
[95] In argomento si vedano le riflessioni di FASANO, L.M., «Le competenze digitali dei dipendenti pubblici: una sfida per la ripresa del paese», in *Agenda Digitale*, 21 settembre 2021, in https://s.uniupo.it/px76x.

del disegno di legge recante disposizioni in materia di reati informatici e di rafforzamento della cybersicurezza nazionale del 23 gennaio 2024[96].

Le Istituzioni pubbliche sono consce della necessità di intervenire per contrastare questo fenomeno. A tal fine, sono state predisposti e adottati sia a livello europeo sia a quello nazionale, specifici piani strategici volti a incrementare il livello di alfabetizzazione digitale dei cittadini: importanti esempi sono rappresentati, ad esempio, oltre al *Next Generation EU* e al PNNR[97], dal *Digital Education Action Plan 2021-2027*[98], dalla Strategia Nazionale per le Competenze Digitali[99], o dalla Strategia per l'innovazione tecnologica e la digitalizzazione del Paese 2025[100], affiancati coerentemente dallo stanziamento di apposite risorse[101].

La strada per raggiungere simili risultati, ambiziosi ma necessari, è lunga e richiede visione strategica e risorse, oltre che pazienza e consapevolezza di imprevisti e di effetti di sistema. Ma d'altronde, come ha scritto Antonio Machado, "*Caminante, son tus huellas / el camino, y nada más; / caminante, no hay camino: / se hace camino al andar*"[102].

[96] Si rimanda alla nota 29.
[97] Sulla base del quale è stata adottata la Direttiva del Ministero della Pubblica Istruzione "Pianificazione della formazione e sviluppo delle competenze funzionali alla transizione digitale, ecologica e amministrativa promosse dal Piano Nazionale di Ripresa e Resilienza", 2023, in https://s.uniupo.it/gu1u7.
[98] Che si pone nel solco sia del Next Generation EU sia della strategia della Commissione Un'Europa pronta per l'era digitale: cf. https://s.uniupo.it/jfdjx.
[99] Cf. https://s.uniupo.it/yq4zo.
[100] Cf. MINISTERO PER L'INNOVAZIONE TECNOLOGICA E LA DIGITALIZZAZIONE, *Strategia per l'innovazione tecnologica e la digitalizzazione del Paese 2025. Le prime azioni per l'Italia del futuro*, 2021, in https://s.uniupo.it/691a8.
[101] Si pensi, ad esempio, al protocollo d'intesa sottoscritto nel 2022 tra Ministero per l'Innovazione Tecnologia e la Digitalizzazione, il Ministero dell'Economia e delle Finanze e l'Associazione di Fondazioni e di Casse di Risparmio Spa, con il quale è stato dato vita al Fondo per la Repubblica Digitale, che ha previsto lo stanziamento di 350 milioni di euro per gli anni 2022-2026. Cf. https://s.uniupo.it/h4gq5.
[102] MACHADO, A., *Campos de Castilla, estratto da Proverbios y Cantares*, XXIX, Siviglia 1912.