Economie dei dati, nuovi poteri ed autorità amministrative: il caso dell'Agenzia per la cybersicurezza nazionale*

Agostino Sola

Abstract

Le economie data driven hanno mostrato un ruolo assolutamente nuovo dei dati, tanto nella creazione delle relazioni economiche quanto nel determinare la forza economica di un'impresa. Questa nuova consapevolezza sta portando all'applicazione di regole specifiche, anche nuove, incentrate sul rapporto tra innovazione e diritto. Nel diritto amministrativo, le economie *data driven* stanno sollevando alcuni interrogativi su quale norma debba essere applicata e da quale autorità: è nota, ad esempio, la correlazione emergente e inaspettata tra diversi ambiti del diritto (privacy, antitrust, cybersicurezza, proprietà intellettuale, per citarne alcune). Le economie *data driven* stanno determinando un'inedita combinazione di poteri e competenze amministrative, individuandone anche di nuove, come è la cybersicurezza. In questo senso, si descrive l'evoluzione del contesto normativo che ha portato alla creazione di un organismo amministrativo assolutamente nuovo al fine di tutelare questo nuovo emergente interesse pubblico per la cybersicurezza: l'Agenzia per la Cybersicurezza Nazionale (ACN).

It is a fact that data driven economies have shown a new role of data in the creation of economic relationships and in determining the economic strength of a company. This new awareness of economic value is leading to the application of specific rules, even new ones, focusing on the relationship between innovation and law. From an administrative perspective, data driven economies are raising some questions about which rule should be applied and by which authority: it is known, for example, the emerging and unexpected correlation between different fields of law: privacy and antitrust but also data retention and cybersicurezza. This phenomenon is representing not only a national but already an European concern. In Italy, following this path, could be observed the growing interest in cybersicurezza that has led to the creation of a new administrative body to protect this newly emerged public interest in cybersicurezza: the Agency for National Cybersicurezza.

* Su determinazione della direzione, il contributo è stato sottoposto a referaggio anonimo in conformità all'art. 15 del regolamento della Rivista

Sommario

Keywords

economia dei dati – cybersicurezza – competenze amministrative - Agenzia per la Cybersicurezza Nazionale

1. Introduzione. L'attuale indiscussa centralità dei dati e le economie dei dati

L'attuale contesto socioeconomico è ormai caratterizzato dall'intervenuta creazione e dal crescente sviluppo di sistemi decisionali, pubblici e privati, basati sull'analisi dei dati, che hanno portato alla definizione della nostra epoca quale oggetto della cd. quarta rivoluzione industriale[1]. Tale rivoluzione si riferisce, in particolar modo, alla circostanza in base alla quale tutti gli ambiti della vita sociale ed economica sono influenzati, direttamente o indirettamente, dalle nuove tecnologie digitali che, con l'avvento e la diffusione di Internet, hanno determinato nuove modalità di comunicazione ed elaborazione dei dati ed una costante interconnessione della popolazione.

Dall'attuale disponibilità di dati[2] e dalle capacità tecnologiche[3] acquisite negli ultimi anni si sono sviluppate le economie dei dati le quali si caratterizzano, in via di prima approssimazione, per l'utilizzo, *recte* lo sfruttamento, di dati, personali e non, all'interno di processi decisionali, tanto pubblici quanto privati, con la finalità di contribuire all'efficienza e alla qualità dei processi produttivi tradizionali ovvero di qualificare in termini di innovazione (anche intesa come personalizzazione) l'offerta di beni e ser-

[1] Secondo K. Schwab – P. Pyka, *Die Vierte Industrielle Revolution*, München, 2016, richiamato da A. Lalli, Il sapere e la professionalità dell'amministrazione pubblica nell'era dei big data e dell'intelligenza artificiale, in *aipda.it*, relazione al Convegno AIPDA 2019.

[2] Il volume dei dati prodotti a livello mondiale è in rapida crescita, dai 33 zettabyte del 2018 ai 175 zettabyte previsti nel 2025 (Report IDC 2018, richiamato nella Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni, *Una strategia europea per i dati*, COM(2020) 66 final, 12 febbraio 2020, 2). Occorre osservare anche che i dati e le informazioni crescono ad una velocità vertiginosa tale da creare un ambiente saturo di dati, in tal senso D.U. Galetta, *La pubblica amministrazione nell'era delle ICT: sportello digitale unico e intelligenza artificiale al servizio della trasparenza e dei cittadini?,* in *Ciberspazio e diritto,* 3, 2018, 327, riporta alcuni dati in tema di aumento del volume delle informazioni disponibili.

[3] Senza adeguata tecnologia, infatti, l'acquisizione di grandi quantità di dati – inintelligibili alla conoscenza umana - rimarrebbe fine a se stessa e priva di qualsiasi utilità pratica e, quindi, di rilevanza economica. La rilevanza dei *big data* è comunque tale da aver portato alla creazione di modelli di business concentrati unicamente nella raccolta e nell'analisi degli stessi.

vizi, digitali e non.[4]

I dati, dunque, al pari delle tecniche algoritmiche di analisi[5], rappresentano ormai un fattore di produzione[6] ed una risorsa economica di fondamentale importanza nell'organizzazione delle attività di produzione e di scambio[7].

L'accennato fenomeno, che ha preso il nome di data driven innovation, non ha interessato soltanto i tradizionali modelli economici[8] ma ha altresì portato alla nascita di particolari sistemi economici che ruotano attorno all'ecosistema dei big data[9].

2. Il nuovo ruolo della cybersicurezza nelle società digitali

La centralità dei dati, unitamente all'utilizzo di risorse tecnologiche, ha sollevato inedite questioni ordinamentali in risposta alle quali si iniziano ad osservare, anche a livello europeo, primi esempi di politiche di regolamentazione *ex ante* sulla loro circolazione ed utilizzo i cui prodotti normativi assumono ormai una forma definitiva[10].

---

[4] In tema si veda il Rapporto OECD, *Data-Driven Innovation. Big Data for Growth and Well-Being*, in *oecd-ilibrary.org*, 6 ottobre 2015.

[5] Ed infatti, se sono gli algoritmi di calcolo che rendono possibile l'inedito sfruttamento di dati deve osservarsi che la disponibilità di nuovi e aggiornati dati consente, a loro volta, il miglioramento degli algoritmi. Dati e algoritmi, dunque, si manifestano sinergicamente connessi non solo quantitativamente ma anche qualitativamente. Il valore dei dati, infatti, dipende non già dalla loro quantità, bensì dalla loro qualità, intesa quale possibilità di estrarre informazioni utili e rilevanti. La disponibilità di dati, in chiave antitrust, non è affatto idonea a determinare *ex se* una posizione dominante nel mercato di riferimento. Ed è proprio su tale deduzione, unitamente ad altre argomentazioni, che si radica lo scetticismo, se non la contrarietà, della dottrina avverso l'obbligo di garantire l'accesso a terzi concorrenti dei dati detenuti dalle imprese. In tema si veda A. Preta – L. Zoboli, *Profili regolatori e concorrenziali in tema di accesso e condivisione dei dati,* in *Analisi Giuridica dell'Economia,* 1, 2019, 213 ss.

[6] Tale locuzione non è casuale ma intende sottolineare l'impiego dei big data nei processi di produzione di altri beni (informazioni rilevanti da questi estratti) successivamente utilizzati per l'offerta di beni e servizi.

[7] In particolare, pare rilevante l'individuazione di due grandi categorie di imprese *data driven*, tanto nei settori ICT quanto in quelli tradizionali: chi fornisce beni e servizi basandosi sui dati raccolti, sia autonomamente sia mediante *data brokers* (*i*); chi fornisce beni e servizi al fine di generare altri dati al fine di migliorare l'esperienza di consumo e per fornire servizi aggiuntivi (*ii*). In tal senso, P. Hartmann – M. Zaki – N. Feldman – A. Neely, *Big data for big business? A taxonomy of data-driven business models used by start-up firms*, in *cambridgeservicealliance.eng.cam.ac.uk*, marzo 2014.

[8] Si tratta, se si vuole, dell'utilizzo analogico dei dati digitali che si ha laddove il prodotto finale non presenta elementi digitali ma, tramite il perfezionamento delle tradizionali catene di produzione, la produzione viene migliorata in termini qualitativi e quantitativi. In termini analoghi, ad esempio, si discute dell'utilizzo di big data per risolvere l'annoso problema delle perdite della rete idrica nazionale (pari al 42% del volume di acqua immesso nella rete, secondo ISTAT, *Censimento delle acque per uso civile* per l'anno 2018, in *istat.it*, 10 dicembre 2020).

[9] Nonostante non vi sia una definizione univoca di *big data,* si preferisce richiamare la definizione a carattere meramente descrittivo in OECD, *Executive Summary of the Competition Committee Roundtable on Big Data,* in *one.oecd.org*, 26 aprile 2017, secondo cui «*Big Data is commonly understood as the use of large scale computing power and technologically advanced software in order to collect, process and analyse data characterised by a large volume, velocity, variety and value*».

[10] Il riferimento è alle iniziative intraprese dalla Commissione europea ha iniziato il proprio percorso verso un approccio globale all'economia dei dati, riconosciuti quale elemento centrale di tutti i sistemi economici e delle società innovativi e moderni, e quale vera e propria «linfa vitale dello sviluppo

Le economie dei dati e le nuove possibilità offerte dall'evoluzione tecnologica, inoltre, stanno influenzando la quotidianità dei rapporti giuridici[11] e, per quanto d'interesse, anche le modalità con cui operano gli Stati in risposta alla necessità di regolazione di fenomeni inediti. In particolare, la rinnovata esigenza di un intervento pubblico si sta innestando su norme e competenze tradizionali alle quali se ne iniziano ad aggiungere di nuove.

Un aspetto di indubbia novità relativo alla risposta degli Stati a tale necessità è offerto dalla crescente attenzione per i profili inerenti alla cybersicurezza, la cui vulnerabilità è stata resa evidente con la diffusione della digitalizzazione.

La cybersicurezza, infatti, viene invocata al fine di garantire l'affidabilità e la sicurezza di quelle attività[12], pubbliche e private, aventi carattere economico ovvero sociale, che vengono svolte mediante utilizzo di tecnologie digitali e, in generale, nello "spazio cibernetico"[13]. L'erogazione di beni e servizi, infatti, è sempre più mediata da piat-

economico» (così come nella Comunicazione COM(2020) 66, cit.). Va ricordato che sin dal 2014, la Commissione ha intrapreso una serie di iniziative per facilitare lo sviluppo di un'economia agile basata sui dati, quali il regolamento sulla libera circolazione dei dati non personali (regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, GU L 303/59); il regolamento sulla cibersicurezza (regolamento (UE) 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»), GU L 151/15); la direttiva sui dati aperti (direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (rifusione), GU L 172/56); il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), GU L 119/1). Nel 2018, ancora, viene presentata per la prima volta una strategia per l'intelligenza artificiale, concordando un piano coordinato con gli Stati membri. La creazione di un contesto normativo di disciplina della risorsa economica dei dati faciliterà altresì l'adozione di primi strumenti di regolazione dell'intelligenza artificiale, basata principalmente sulla capacità di analisi dei dati raccolti e sul punto, allora, pare di interesse ricordare che, nelle sue comunicazioni del 25 aprile 2018 e del 7 dicembre 2018, la Commissione europea ha definito la sua visione a sostegno di un'intelligenza artificiale che sia «etica, sicura e all'avanguardia realizzata in Europa». Ed ancora, in European Group on Ethics in Science and New Technologies, *Statement on Artificia, Robotics and 'Autonomous' Systems*, in *op.europa.eu*, 9 marzo 2018, presentato alla Commissione, sono individuati nove «principi etici e requisiti pre-democratici» che dovrebbero fornire una guida futura per legislatori, regolatori e giudici: dignità umana; autonomia; responsabilità; giustizia, equità e solidarietà; democrazia; *rule of law and accountability*; sicurezza, integrità fisica e mentale; protezione dei dati e privacy; sostenibilità.

[11] Le rivoluzioni scientifiche e tecnologiche contribuiscono a modificare i paradigmi sociali e, quindi, giuridici: portano a trasformazioni anche radicali della società umana e, conseguentemente, del contesto normativo di riferimento. Si pensi, ad esempio, alle questioni di bioetica che il progresso scientifico ha sollevato.

[12] Come osservato da A. Tina, *Cybersicurezza: integrità dei processi e dei dati*, in M. Cian – C. Sandei (a cura di), *Diritto del Fintech*, Padova, 2020, 103, i rischi per le imprese, legati ad un *cyber attack,* possono essere così enucleati: *privacy liability* (1); *network security liability* (violazione rete aziendale) (2); *media liability* (violazione copyright) (3); interruzione di attività – malfunzionamenti (4); data asset loss (5); *cyber extortion* (6); *cyber crime* (7).

[13] In via di prima approssimazione potremmo definire l'oggetto della disciplina relativa alla cybersicurezza come quello "spazio cibernetico" formato dalle infrastrutture informatiche, *hardware* e *software,* interconnesse tra loro e attraverso le quali circolano dati e nelle quali si relazionano utenti. In particolare, nello spazio cibernetico si ricomprende internet, le reti di comunicazioni, i sistemi di

taforme e servizi digitali. Reti e sistemi informativi non coinvolgono solamente le economie digitali ma sono essenziali per il funzionamento anche di molte imprese tradizionali che fondano le proprie strategie di mercato proprio sull'utilizzo di tali servizi digitali.

Da tale interdipendenza deriva la necessità di garantire – tramite idonee misure di cybersicurezza - la sicurezza, la continuità e l'affidabilità delle reti e dei sistemi informativi mediante i quali vengono offerti servizi digitali su cui fanno sempre più affidamento molte imprese.

In termini più generali, come già osservato a livello globale[14], si sta assistendo alla comparsa di nuove minacce alla sicurezza che, in quanto tali, richiedono risposte inedite in grado di salvaguardare la spinta innovativa delle economie data driven.

Tra i profili di rischio legati alla cybersicurezza si devono tenere in considerazione anche i sistemi aggregati di conservazione di dati, necessari per le attuali tecnologie algoritmiche, ed in relazione ai quali continua a trovare applicazione la disciplina europea di protezione dei dati personali.[15]

La necessità di una adeguata risposta alle nuove minacce derivanti dalla diffusione delle tecnologie digitali ha determinato una rinnovata sensibilità per gli aspetti propri della cybersicurezza tanto in relazione al corretto funzionamento dei sistemi informativi quanto in relazione al possibile coinvolgimento di dati personali.

L'erogazione di beni e servizi mediante l'utilizzo di infrastrutture digitali ha manifestato il bisogno che queste siano rese affidabili e sicure a vantaggio tanto degli utenti dei servizi digitali quanto degli operatori coinvolti. L'aumento delle infrastrutture digitali e la crescente accessibilità a strumenti informatici e digitali hanno condotto, nell'ultimo decennio, a sempre più frequenti attacchi cibernetici, dovuti anche alla scarsità (in termini qualitativi e quantitativi) dei mezzi di difesa.[16]

La creazione e il mantenimento di uno spazio digitale capace di offrire adeguate garanzie di sicurezza, infatti, rappresenta una condizione necessaria per fruire pienamente delle possibilità, in parte ancora inesplorate, offerte dal progresso tecnologico. Viceversa, le garanzie di sicurezza consentono altresì di evitare l'esposizione a rischi sistemici rovinosi per lo Stato, ad oggi ancora il principale obiettivo degli attacchi ci-

elaborazione dati e i *dispositivi* attraverso cui si accede alla rete. Ad oggi, la *cybersicurezza* viene definita dalla legislazione europea (regolamento (UE) 2019/881, cit., art. 2, n. 1) quale «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche».

[14] OECD, *Data-Driven Innovation,* cit., 40.

[15] Con particolare riferimento alla Sezione II del regolamento (UE) 2016/679, cit. (GDPR) in tema di misure di sicurezza da adottare qualora siano coinvolti dati personali. E ciò indipendentemente dalla conservazione dei dati per finalità pubblicistiche (*public data retention*), anche a carattere securitario.

[16] In particolare, per una visione d'insieme si deve osservare Presidenza del Consiglio dei Ministri – Sistema di Informazione per la Sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2021*, in *sicurezzanazionale.gov.it*, febbraio 2022. In particolare, viene osservata una tendenza in crescita delle attività ostili per la sicurezza cibernetica: nel corso del 2021, ad esempio, maggiormente colpite sono le infrastrutture informatiche della Pubblica Amministrazione (69%, in diminuzione di 14 punti percentuali rispetto al 2020), perlopiù Amministrazioni Centrali dello Stato (56%, valore in aumento rispetto all'anno precedente) e infrastrutture IT riferibili a enti locali e strutture sanitarie (pari a circa il 30%). In ambito privato, sono stati interessati prevalentemente i settori energetico (24%), dei trasporti (18%) e delle telecomunicazioni (12%).

bernetici.

In termini più generali, dunque, in ragione del crescente utilizzo delle tecnologie informatiche, la cybersicurezza non è più solo limitata a settori strategici per la sicurezza nazionale (difesa militare, infrastrutture essenziali, telecomunicazioni) ma coinvolge l'intero mercato e trova un'applicazione generalizzata a tutte quelle attività economiche e sociali che si svolgono mediante l'utilizzo della rete e dei sistemi informativi. Tratto distintivo della cybersicurezza è che, tutelando il proprio interesse primario, finisce per rappresentare anche distinti ed ulteriori interessi di carattere pubblicistico. Occorre però notare che la cybersicurezza non garantisce solamente il corretto funzionamento delle attività economiche e sociali che si svolgono mediante l'utilizzo della rete e dei sistemi informativi ma rappresenta uno strumento di tutela eterogenea. È chiara, dunque, l'interdisciplinarietà della cybersicurezza che, nel tutelare il proprio interesse primario, finisce per rappresentare anche distinti ed ulteriori interessi di carattere pubblicistico. In particolare, modo, ad esempio, la cybersicurezza, nel garantire l'inviolabilità delle reti, tutela altresì i dati digitali che in queste sono conservati. Dati digitali che, spesso, hanno carattere personale e per i quali si rende necessaria una particolare tutela che tenga altresì in considerazione la specifica normativa sui dati personali. La disciplina di sicurezza delle reti non esclude l'applicazione delle regole poste a protezione dei dati personali che prevedono l'adozione di «misure tecniche e organizzative adeguate» [17] tali da evitarne trattamenti non autorizzati, e, quindi, illeciti. La portata degli obblighi previsti dalla disciplina della protezione dei dati personali, è stato già osservato[18], è in larga parta sovrapponibile alla disciplina sulla cybersicurezza: senza pretesa di esaustività, si consideri che entrambi le discipline prevedono misure di sicurezza "adeguate" alla gestione del rischio e tra queste rientra, ormai, anche la gestione del rischio *cyber*.

Ad oggi, la rinnovata consapevolezza della pericolosità del fenomeno ha oggi portato il legislatore nazionale ed europeo ad ideare una strategia normativa al fine di assicura-

[17] Così prevede l'art. 5, regolamento (UE) 2016/679, cit. in tema di principi applicabili al trattamento dei dati personali, da leggere unitamente all'art. 24 sulla responsabilità del titolare del trattamento dei dati personali.

[18] In particolare, M. Giordano – I. Oldani – M. Simbula, *Principi di sicurezza applicabili ai cloud computing services: GDPR, Direttiva NIS e PSD2 a confronto*, in *Ciberspazio e diritto*, 1, 2020, 123; A. Tina, *Cybersicurezza,* cit., 99 e, sulla complementarità delle due discipline, M. Viggiano, *Cybersicurezza and Data Protection in European Union Policies and Rules: The NIS Directive anche the GDPR Synergy*, in G. De Minico – O. Pollicino (a cura di), *Virtual freedoms terrorism and the law,* Torino, 2020, 63 ss. Ancora, sul rapporto tra *privacy* e cybersicurezza è interessante richiamare una guida dell'autorità inglese per la protezione dei dati personali: ICO, *NIS and the UK GDPR*, in *ico.org.uk*. Lo stesso considerando 63 della direttiva NIS (direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, GU L 194/1) osserva la possibile compromissione di dati personali a seguito di evento con un impatto sulla sicurezza della rete e dei sistemi informativi ragion per cui, poi, nel corpo della Direttiva si delinea, una rete di collaborazione e scambio di informazioni tra autorità e si prevedono «ove opportuno e conformemente al diritto nazionale» (art. 8) consultazioni e collaborazioni tra le autorità competenti e le autorità per la protezione dei dati nazionali. Ad oggi, tale direttiva è stata sostituita per effetto dell'entrata in vigore della 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), GU L 333/80.

re *ex ante* la tenuta cibernetica dei sistemi digitali così da limitare le possibilità di attacco, diversamente dalle prime disposizioni in materia che, complice l'assoluta novità del fenomeno, si concentravano su una «difesa, per ora, di tipo prevalentemente - anche se non esclusivamente - reattivo»[19].

3. La cybersicurezza: evoluzione normativa europea

La centralità dei dati, unitamente all'utilizzo di risorse tecnologiche, ha sollevato inedite questioni ordinamentali in risposta alle quali si osserva, anche a livello europeo, un esempio di regolazione trasversale della materia. In particolare, si osserverà l'evoluzione della disciplina della cybersicurezza.

Il legislatore europeo, nonostante l'attenzione per la sicurezza delle infrastrutture dell'informazione fosse già stata evidenziata sin dai primi anni 2000[20], ha iniziato a tratteggiare una prima architettura regolamentare con la "*Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*" (JOIN(2013) 1 final, 7 febbraio 2013)[21] e la contestuale proposta di direttiva sulla sicurezza delle reti e dell'informazione che vedrà la luce con la nota direttiva 2016/1148/UE (cd. direttiva NIS).

La direttiva NIS definiva un livello comune di intervento europeo a protezione delle infrastrutture critiche anche mediante inediti schemi e modalità di cooperazione internazionale. L'elemento caratterizzante era l'indicazione di una prima base normativa unitaria in un panorama piuttosto eterogeneo e diversificato[22].

---

[19] Presidenza del Consiglio dei ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, in *agid.gov.it*, dicembre 2013, 11.

[20] In particolare, si fa qui riferimento alla Comunicazione della Commissione europea al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni, *Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica,* COM/2000/0890 def., 26 gennaio 2001. Come ricorda C. Cencetti, *Cybersicurezza: Unione europea e Italia. Prospettive a confronto,* Roma, 2014, nella fase iniziale le politiche europee si sono concentrate sulla sicurezza delle infrastrutture critiche, sulla protezione dei dati personali e sulla repressione dei crimini *cyber*. Si deve menzionare altresì l'istituzione dell'ENISA, l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, con regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione, GU L 77/1, al fine di «assicurare un alto ed efficace livello di sicurezza delle reti e dell'informazione nell'ambito della Comunità e di sviluppare una cultura in materia di sicurezza delle reti e dell'informazione» nonché di «assiste[re] la Commissione e gli Stati membri, e di conseguenza collabora con la comunità degli operatori economici». Il regolamento è stato poi abrogato e sostituito dal regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004, GU L 165/41. Ad oggi, per effetto del regolamento (UE) 2019/881, cit., il ruolo dell'ENISA è ancora più centrale per la promozione di un elevato livello di cybersicurezza e cyber-resilienza.

[21] Per un interessante ed esaustivo commento si rinvia a M. Bassini, *Cybersicurezza*, in M. Paracampo (a cura di), *Fintech*, Vol. I, Torino, 2021, 321 ss.

[22] E ciò con evidente compromissione del livello globale di sicurezza delle reti e dei sistemi informativi in Europa, sino ad allora solo in parte mitigato dalle linee guida ENISA. In questo senso, la direttiva NIS, nell'istituire le misure necessarie alla creazione di «un livello comune elevato di sicurezza delle reti e dei sistemi informativi» compiva un rilevante sforzo definitorio nell'individuare le nozioni comuni di "rete e sistema informativo" e la relativa "sicurezza della rete e dei sistemi informativi", fornendone un primo approccio unitario e ripreso poi dalla direttiva NIS 2, direttiva (UE) 2022/2555, cit.

Ad oggi, tale direttiva è stata sostituita per effetto dell'entrata in vigore della Dir. 2022/2555/UE "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)".[23] L'obbligo di recepimento della Direttiva NIS 2 (direttiva 2022/2555/UE) viene indicato al 17 ottobre 2024: dal giorno successivo sarà abrogata la direttiva 1016/1148/UE.
In ragione dell'espansione del panorama delle minacce informatiche, si è esteso l'ambito di applicazione della Direttiva NIS 2 che oggi risulta più ampio ed omogeno: da una parte, infatti, si rivolge anche a soggetti pubblici[24]; dall'altra, supera la differenziazione tra gli operatori di servizi essenziali e i fornitori di servizi digitali, propria della precedente direttiva e ritenuta ormai «obsoleta»[25]. Le disposizioni in materia di cybersicurezza trovano applicazione nei confronti di quelle imprese che operano in settori ritenuti critici[26] e i soggetti privati cui la direttiva si riferisce sono suddivisi in

[23] La modifica della disciplina in materia è parte delle azioni indicate nella più ampia strategia digitale europea. In tema, sulla strategia digitale europea, con particolare riferimento alle economie dei dati, sia consentito il rinvio ad A. Sola, *Primi cenni di regolazione europea nell'economia dei dati*, in questa *Rivista,* 3, 2021, 188 ss. La modifica della direttiva NIS è mossa dal dichiarato fine di «rafforzare l'autonomia strategica dell'Unione per migliorarne la resilienza e la risposta collettiva e creare una rete Internet globale e aperta» sulla scorta dell'impatto subìto in termini di adeguatezza ed aderenza all'attuale digitalizzazione ed interconnessione dei servizi chiave all'economia e alla società.

[24] In particolare, agli enti della pubblica amministrazione centrale e regionale (ma, questi ultimi, solo qualora risulti che forniscono «servizi la cui perturbazione potrebbe avere un impatto significativo su attività sociali o economiche critiche»). Così, l'art. 2, c. 2, lett. f, della direttiva NIS 2, direttiva (UE) 2022/2555, cit. È rimessa alla discrezionalità del legislatore nazionale la scelta di estendere l'ambito di applicazione delle norme in materia anche alle amministrazioni locali ed agli istituti di istruzione. Sono escluse le amministrazioni pubbliche nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa, del contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati.

[25] In questi termini, al considerando 6 della Direttiva NIS 2, direttiva (UE) 2022/2555, cit. Il precedente impianto normativo offerto dalla direttiva NIS distingueva, ai fini dell'applicazione delle regole ivi contenute, tra "operatori di servizi essenziali" e i "fornitori di servizi digitali", sottoposti a distinti obblighi preventivi in materia di sicurezza e di controlli successivi tramite l'obbligo di notifica degli incidenti. In particolare, ai sensi dell'art. 5, direttiva (UE) 2016/1148, cit., si consideravano "operatori di servizi essenziali" quanti forniscano un servizio «essenziale per il mantenimento di attività sociali e/o economiche fondamentali» (a); la cui fornitura dipende dalla rete e dai sistemi informativi (b); e in caso di incidente si avrebbero «effetti negativi rilevanti sulla fornitura di tale servizio» (c). Erano invece "fornitori di servizi digitali", secondo quanto previsto dall'Allegato III, le imprese che operano nei mercati online (*marketplace*), che forniscono servizi di motori di ricerca online e che offrono servizi di *cloud computing*.

[26] In particolare, secondo l'Allegato II alla Direttiva NIS 2, direttiva (UE) 2022/2555, cit., si riconoscono "settori ad alta criticità", con un'elencazione che amplia quella degli "operatori di servizi essenziali" di cui alla precedente direttiva. In particolare, rientrano in questa categoria le imprese che operano nei settori dell'energia (elettricità, teleriscaldamento e teleraffrescamento, petrolio, gas, idrogeno), del trasporto (aereo, ferroviario, portuale, stradale), bancario, delle infrastrutture dei mercati finanziari, sanitario, della distribuzione dell'acqua potabile, della gestione delle acque reflue, delle infrastrutture digitali, di gestione dei servizi di telecomunicazione (*business-to-business)*, amministrazioni pubbliche e, da ultimo, di fornitura di servizi spaziali. Secondo l'Allegato III alla Direttiva NIS 2, direttiva (UE) 2022/2555, cit., si riconoscono come "altri settori critici" quelle imprese che operano nei settori dei servizi postali e di corriere, della gestione dei rifiuti, industria chimica (fabbricazione, produzione e distribuzione di sostanze chimiche), industria alimentare (produzione, trasformazione e distribuzione di alimenti), fabbricazione di dispositivi medici, fabbricazione di computer e prodotti di elettronica e ottica, fabbricazione di apparecchiature elettriche, fabbricazione di macchinari e apparecchiature n.c.a., fabbricazione di mezzi di trasporto, fornitori di servizi digitali e organizzazione di ricerca.

"essenziali" ed "importanti"[27].

Riprendendo quanto già previsto dalla precedente direttiva, la Direttiva NIS 2 prevede l'obbligo per gli Stati di adottare una "Strategia nazionale per la cibersicurezza", mediante l'adozione di uno o più strumenti legislativi o non legislativi. Tale atto programmatico, al netto dello specifico contenuto delle «misure strategiche e normative al fine di raggiungere e mantenere un livello elevato di cibersicurezza» [28], si viene ad arricchire di nuovi contenuti e diventa strumento centrale per garantire l'efficace coordinamento tra le autorità coinvolte, non soltanto a livello internazionale[29] ma anche, e, soprattutto, a livello nazionale.[30]

Gli attori istituzionali coinvolti a livello nazionale si ispirano a quelli già indicati dalla precedente direttiva (e già operativi nei singoli Stati): un'autorità competente responsabile della cibersicurezza e dei compiti di vigilanza che svolge anche le funzioni di

[27] La prima categoria viene puntualmente definita dall'art. 3, c. 1, della Direttiva NIS 2, direttiva (UE) 2022/2555, cit. La seconda, invece, viene definita in negativo come «soggetti di una tipologia elencata negli allegati I o II che non sono considerati soggetti essenziali» (art. 3, c. 3). Così come il precedente quadro normativo, i soggetti privati cui la direttiva si riferisce sono individuati in un elenco tenuto ed aggiornato ad opera dei singoli Stati. Si prevede, tuttavia, l'inedita possibilità per gli stati di indicare le modalità di registrazione autonoma dei soggetti.

[28] L'ambito di riferimento di tali "misure strategiche" viene puntualmente declinato dalla Direttiva NIS 2, direttiva (UE) 2022/2555, cit., laddove, invece, la precedente direttiva NIS, direttiva (UE) 2016/1148, non forniva indicazioni in tal senso e, di fatto, determinava una forte disomogeneità sul territorio europeo in grado di pregiudicare la tenuta del sistema di sicurezza. Tra le varie misure strategiche indicate si segnalano misure di prevenzione ed educazione alla cybersicurezza ed alla cyber-resilienza (*cyber hygiene*). Le strategie nazionali devono essere poi valutate ed aggiornate periodicamente.

[29] Il coordinamento "strategico" a livello internazionale è garantito dall'istituzione di un gruppo di cooperazione (art. 14, direttiva (UE) 2022/2555, cit.), già previsto dalla precedente disciplina, e composto da rappresentanti degli Stati membri, della Commissione e dell'ENISA. Allo scopo di garantire un coordinamento "operativo" rapido ed efficace tra Stati membri viene, invece, istituita una "rete dei CSIRT nazionali" (art. 15, direttiva (UE) 2022/2555, cit.), già prevista dalla precedente disciplina. Al fine di una gestione coordinata degli incidenti sul territorio europeo, viene creata una rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) (art. 16, direttiva (UE) 2022/2555, cit.) formata da rappresentanti delle autorità di gestione delle crisi informatiche degli Stati membri e, nei casi più gravi, anche dalla Commissione. Al fine di contribuire allo sviluppo della fiducia e di promuovere una cooperazione operativa rapida ed efficace fra gli Stati membri, è istituita una rete dei CSIRT nazionali.

[30] L'architettura generale del coordinamento in materia risulta analoga alla precedente e si mantiene un sistema capillare di autorità nazionali competenti, punti di contatto unici a livello nazionale e CSIRT, in coordinamento tra loro. Si prevede l'indicazione delle misure di coordinamento specifiche conseguenti alla relazione tra le disposizioni in materia di cybersicurezza e le normative di settore. In particolare, infatti, si prevede che queste ultime trovino applicazione prioritaria solo qualora siano "almeno equivalenti", pur dovendo garantire «la coerenza e l'efficacia del trattamento delle notifiche degli incidenti» tra autorità. Oggetto di richiamo puntuale, tra le normative di settore dell'Unione, è quella relativa ai soggetti finanziari contemplati dal regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (c.d. regolamento DORA) nei cui confronti non trovano applicazione le disposizioni in materia di cybersicurezza. Al contrario, invece, ai soggetti identificati come soggetti critici a norma della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio del 14 dicembre 2022 del Parlamento europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio, GU L 333/164, si applicano le disposizioni in materia di cybersicurezza e sono considerati soggetti essenziali (esclusi gli operatori del settore delle infrastrutture digitali).

punto di contatto unico[31]; quadri nazionali di gestione delle crisi informatiche;[32] gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)[33].

Le misure indicate dalla Direttiva NIS 2 al fine di garantire la sicurezza dei sistemi informatici e di rete sono principalmente due: l'attuazione di strumenti per la gestione del rischio di cibersicurezza ed il rispetto degli obblighi di segnalazione.[34] Come già osservato, i soggetti tenuti all'applicazione della disciplina in materia sono quelli considerati "essenziali" ed "importanti".

La gestione dei rischi di cybersicurezza, indicata dall'art. 21, direttiva 2022/2555/UE, trova attuazione mediante l'adozione di misure tecniche, operative e organizzative che siano "adeguate e proporzionate" alle specificità del soggetto.[35] Si incoraggia, in questi termini, l'adozione di ogni tecnologia innovativa, compresa l'intelligenza artificiale, il cui utilizzo potrebbe migliorare l'individuazione e la prevenzione degli attacchi informatici.

In particolare, le misure di gestione dei rischi devono risultare adeguate ai rischi esistenti e proporzionate alla tipologia di attività svolta. L'approccio da adottare è definito "multirischio".

L'obbligo di notifica di incidenti, invece, indicato dall'art. 23, direttiva 2022/2555/UE, impone la comunicazione "senza indebito ritardo", rapida ma approfondita, al

---

[31] In particolare, l'autorità competente (o il punto di contatto unico in caso di più autorità competenti) svolge una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità del relativo Stato membro con le autorità pertinenti degli altri Stati membri, e, ove opportuno, con la Commissione e l'ENISA, nonché per garantire la cooperazione intersettoriale con altre autorità competenti dello stesso Stato membro. In Italia, l'autorità competente è l'Agenzia per la cybersicurezza nazionale (ACN), di recente istituzione. In tema, per ulteriori approfondimenti circa i profili organizzativi e funzionali dell'Agenzia si rimanda a L. Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, in *Giornale di Diritto Amministrativo,* 6, 2021, 709 ss.

[32] Si tratta di una o più una autorità responsabili «della gestione degli incidenti e delle crisi di cibersicurezza su vasta scala» (art. 9, direttiva (UE) 2022/2555, cit.) definite anche "autorità di gestione delle crisi informatiche*"*. Non si riscontra una figura analoga nella precedente direttiva che non faceva alcun riferimento alle "crisi informatiche*"*.

[33] Il "Team di risposta agli incidenti di sicurezza informatica", anche definito "*Computer Security Incident Response Team*" da cui l'acronimo inglese "CSIRT*",* svolge funzioni di prevenzione delle minacce informatiche (monitoraggio, assistenza, emissione di preallarmi, analisi preventive sui rischi, "scansione proattiva dei sistemi informatici"), funzioni di risposta e assistenza in caso di incidenti nonché di coordinamento e cooperazione in risposta a incidenti di sicurezza informatica. Il CSIRT si viene ad arricchire anche di nuove funzioni correlate al contrasto alle vulnerabilità dei sistemi informatici e di rete la cui la rapida individuazione e correzione è un fattore importante per la riduzione dei rischi *cyber*. In questo senso, vengono introdotte misure di "divulgazione coordinata delle vulnerabilità" (art. 12, direttiva (UE) 2022/2555, cit.) per segnalarle ai produttori e fornitori così da consentire loro di diagnosticarle ed eliminarle. In questo contesto, il CSIRT svolte funzioni di coordinamento CSIRT come "intermediario di fiducia" tra segnalanti e i fabbricanti o fornitori di prodotti o servizi interessati dalle vulnerabilità. Con l'art. 12, direttiva (UE) 2022/2555, cit., si viene a disporre la creazione di una "banca dati europea delle vulnerabilità", curata e gestita dall'ENISA, al fine di divulgare le vulnerabilità e fornire informazioni su di esse così da consentire agli utenti di adottare adeguate misure di attenuazione. Il CSIRT Italia è istituito presso l'Agenzia per la cybersicurezza nazionale (ACN).

[34] Si riprende e si amplia, anche rendendola unitaria, la previsione di "obblighi in materia di sicurezza e notifica degli incidenti", propri della precedente direttiva.

[35] Al fine di dimostrare l'adeguatezza delle misure di gestione del rischio è possibile fare applicazione di prodotti, servizi e processi certificati nell'ambito dei sistemi europei di certificazione della cibersicurezza previsti dal regolamento (UE) 2019/881, cit., (art. 49). Al medesimo scopo, gli Stati membri possono individuare standard tecnici relativi alla sicurezza dei sistemi informatici e di rete.

proprio CSIRT di eventuali incidenti "significativi" [36] tali da impattare negativamente sulla fornitura dei loro servizi. Analoga comunicazione può essere notificata – ove opportuno – ai destinatari dei servizi interessati. Alla disciplina delle ipotesi di notifica obbligatoria si accompagnano ipotesi di notifica volontaria di incidenti esclusi dall'ambito di applicazione dell'art. 23 ovvero da parte di soggetti esclusi dall'applicazione della Direttiva NIS 2.

Le misure di esecuzione e le funzioni di vigilanza circa l'attuazione delle disposizioni in materia sono riservate alle autorità competenti, in stretto coordinamento con le altre autorità coinvolte[37], anche al fine di evitare duplici sanzioni a fronte delle medesime condotte.[38]

Il regolamento (UE) 2019/881 ("*Cybersecurity Act*") prevede altresì l'introduzione di sistemi europei di certificazione della cybersicurezza, coordinati poi a livello nazionale e volti ad uniformare ulteriormente la risposta preventiva alle minacce *cyber* nel territorio europeo.

4. (segue): panorama normativo nazionale

L'attuale quadro di riferimento normativo è offerto principalmente dal d.lgs. 65/2018 (decreto attuativo della direttiva NIS), dal d.l. 105/2019 istitutivo del perimetro di sicurezza nazionale cibernetica e, più di recente, dal d.l. 82/2021 istitutivo, come si vedrà, dell'Agenzia per la Cybersicurezza Nazionale (ACN).

L'architettura istituzionale di riferimento è influenzata dalla peculiarità degli interessi coinvolti: organi di raccordo verticale a livello internazionale, sistemi orizzontali ed un forte accentramento di poteri. In particolare, poi, il coinvolgimento di interessi di sicurezza nazionale ha imposto una serie di interazioni con il "Sistema di informazione per la sicurezza della Repubblica" ed ha determinato l'accentramento delle funzioni in materia in capo al Presidente del Consiglio dei ministri[39].

La disciplina nazionale in materia di cybersicurezza, al netto della più o meno raggiunta definitività, ha preso le mosse, pur in ritardo, con il D.P.C.M. 24 gennaio 2013

[36] Ai sensi del richiamato art. 23, direttiva (UE) 2022/2555, cit., sono significativi quegli incidenti che causino «una grave perturbazione operativa» dei servizi o perdite finanziarie per il soggetto interessato ovvero ripercussioni su soggetti terzi causando loro «perdite materiali o immateriali considerevoli».

[37] Tra queste, le autorità poste a tutela dei dati personali: in tal senso, infatti, l'art. 31, direttiva (UE) 2022/2555, cit., prevede «nei casi di incidenti che comportano violazioni di dati personali». Specifico riferimento è anche alle autorità competenti sulla vigilanza e sull'esecuzione nei confronti dei soggetti finanziari ai sensi del regolamento (UE) 2022/2554, cit.

[38] In particolare, si fa espresso riferimento alle "violazioni che comportano una violazione dei dati personali": in tal senso, infatti, l'art. 35, direttiva (UE) 2022/2555, cit., prevede specifici obblighi informativi nel caso in cui la violazione degli obblighi imposti in materia di cybersicurezza da parte di un soggetto essenziale o importante possa comportare una violazione dei dati personali. In tali ipotesi le autorità compenti sono tenute ad informare "senza indebito ritardo" le autorità di controllo poste a tutela dei dati personali. Nel caso in cui queste impongano una sanzione amministrativa pecuniaria, le autorità competenti in materia di cybersicurezza si astengono dall'imporre una sanzione amministrativa pecuniaria relativa al medesimo comportamento, già sanzionato.

[39] Al quale l'ACN, come si dirà, sembra avvicinarsi: in tal senso, Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, cit., 719.

"Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale". A tale decreto sono poi seguiti, nello stesso anno, il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico", e il "Piano nazionale per la protezione cibernetica e la sicurezza informatica", successivamente aggiornato nel 2017. Emerge sin da subito la centralità del ruolo del Presidente del Consiglio dei ministri e degli organi della sicurezza nazionale, veri protagonisti in materia di cybersicurezza chiamati ad intervenire tramite il coordinamento degli enti coinvolti a fini di prevenzione, risposta e resilienza dei sistemi di rete nazionali.

L'attuale sistema istituzionale di cybersicurezza trova il proprio fondamento nel D.P.C.M. del 17 febbraio 2017 (c.d. Decreto Gentiloni) "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*"* con cui si è aggiornata l'architettura istituzionale del ricordato D.P.C.M. 24 gennaio 2013 individuando gli attori principali nel Presidente del Consiglio dei Ministri[40], nel Comitato interministeriale per la sicurezza della Repubblica (CISR)[41] – e relativo organo di supporto tecnico[42] - e nel Dipartimento delle informazioni per la sicurezza (DIS)[43]. Si rese, dunque, ancora più evidente lo stretto legame tra il quadro nazionale della governance in materia di cybersicurezza e le strutture coinvolte nelle questioni di sicurezza nazionale.

Sin qui la disciplina viene resa in assenza di fonti primarie e basata, come visto, su provvedimenti di indirizzo e coordinamento degli enti coinvolti.[44] È solo successiva-

[40] Indicato «quale responsabile della politica generale del Governo e vertice del Sistema di informazione per la sicurezza della Repubblica» ed avente le seguenti competenze: convoca il CISR nelle situazioni di crisi che coinvolgono aspetti di sicurezza nazionale; adotta, su proposta del CISR, il quadro strategico nazionale per la sicurezza dello spazio cibernetico; adotta, su delibera del CISR, il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali ed emana le relative direttive di indirizzo ed attuazione; impartisce, sentito il CISR, le direttive necessarie per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali.

[41] In particolare, al CISR erano originariamente riconosciute funzioni di: proposta (con riferimento al quadro strategico nazionale per la sicurezza dello spazio cibernetico); delibera, controllo e attuazione (con riferimento al Piano nazionale per la sicurezza dello spazio cibernetico); indirizzo, collaborazione tra i soggetti istituzionali e gli operatori privati interessati; cooperazione internazionale; proposta di intervento normativo. Con il D.P.C.M. del 17 febbraio 2017 (c.d. Decreto Gentiloni) gli vengono riconosciute anche funzioni di consulenza e di proposta in caso di crisi cibernetica a supporto del Presidente del Consiglio dei ministri. Ad oggi, le competenze del CISR in materia di cybersicurezza sono state trasferite al CIC – Comitato interministeriale per la cybersicurezza (ad esclusione di quelle previste dall'art. 5, d.l. 5/2019).

[42] Istituito con il D.P.C.M. del 17 febbraio 2017, cit., il CISR Tecnico ha funzioni di supporto (preparatorie ed istruttorie) alle ricordate attribuzioni del CISR.

[43] Ai sensi della l. 124/2007 ha principalmente, ma non solo, funzioni di coordinamento per le attività relative alla protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali. All'interno del Dipartimento delle informazioni per la sicurezza (DIS) operano (*recte,* operavano) il punto di contatto unico ai fini dell'applicazione della direttiva NIS, il Nucleo sicurezza cibernetica (NSC), il Computer Security Incident Response Team (CSIRT). Con D.P.C.M. del 17 febbraio 2017, cit., al Dipartimento delle informazioni per la sicurezza (DIS) viene attributo il compito di adottare le linee di azione di interesse generale con l'obiettivo di innalzare e migliorare i livelli di sicurezza dei sistemi e delle reti. Ad oggi, le competenze del DIS in materia di cybersicurezza sono state trasferite in capo all'ACN.

[44] Per una ricognizione dell'evoluzione normativa in materia si richiama A. Renzi, *La sicurezza cibernetica: lo stato dell'arte,* in *Giornale di Diritto Amministrativo,* 4, 2021, 538 ss. e B. Carotti, *Sicurezza cibernetica e Stato-nazione*, in *Giornale di Diritto Amministrativo,* 5, 2020, 629 ss.

mente che, nel recepire la direttiva NIS, 2016/1148/UE, si interviene nella materia con una fonte legislativa primaria, il d.lgs. n. 65/2018 e successivi decreti attuativi. Tra questi, di particolare rilevanza risulta essere il D.P.C.M. 8 agosto 2019, con cui è stato costituito il "Computer Security Incident Response Team" (CSIRT) presso il Dipartimento delle informazioni per la sicurezza della Repubblica, altresì indicato quale punto di contatto unico ai sensi delle ricordate direttive europee. Quanto all'individuazione delle Autorità NIS, invece, si sono indicate nelle strutture ministeriali, con attribuzione di competenze al Ministero dello Sviluppo economico (per i settori energia, infrastrutture digitali e per gli FSD), al Ministero delle Infrastrutture e dei trasporti (per il settore trasporti), al Ministero dell'Economia e delle finanze, in coordinamento con Banca d'Italia e Consob (per i settori bancario e infrastrutture dei mercati finanziari), al Ministero della Salute, alle Regioni e Province autonome di Trento e Bolzano (per il settore sanitario) e, infine, quest'ultime, insieme al Ministero dell'Ambiente e della tutela del territorio e del mare (per il settore della fornitura e distribuzione di acqua potabile).

Da qui, però, la disciplina di riferimento viene ancora una volta a mutare per effetto dell'entrata in vigore del d.l. 105/2019 (convertito, con modificazioni, dalla l. 133/2019). Tale elaborato normativo ha istituito il "perimetro di sicurezza nazionale cibernetica" ed ha riorganizzato l'architettura istituzionale di riferimento in materia. Il perimetro di sicurezza nazionale cibernetica, salutato come inedito strumento ideato dal legislatore nazionale[45], prevede ed assicura un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici all'interno dello stesso perimetro, nel quale si trovano amministrazioni pubbliche, enti ed operatori nazionali, pubblici e privati, dai quali dipende l'esercizio di funzioni essenziali dello Stato[46] e la prestazione di servizi essenziali per gli interessi dello Stato.

All'interno del perimetro possono essere esercitati poteri tipicamente pubblicistici di controllo, ispettivi e sanzionatori da parte delle amministrazioni preposte[47] e sono sottoposti altresì ad una serie di previsioni gravanti direttamente sui soggetti all'interno del perimetro e relative ad attività di prevenzione, di notifica e risposta agli incidenti nonché agli obblighi informativi gravanti sugli stessi[48].

---

[45] Osserva A. Renzi, *La sicurezza cibernetica*, cit., 539 che si tratta di un sistema di protezione cibernetica avanzato di cui non si rinvengono simili neanche nel panorama internazionale: la misura è entrata in funzione per un periodo di prova di sei mesi a partire dal 23 giugno 2021, proprio con la finalità di testarne le debolezze e le peculiarità.

[46] In tema, circa gli interrogativi sollevati dalla nozione di "funzione essenziale dello Stato" si veda B. Carotti, *Sicurezza cibernetica e Stato-nazione*, cit., 632.

[47] Deve essere evidenziato altresì che all'interno del perimetro di sicurezza nazionale cibernetica *ex* d.l. 105/2019, a difesa dell'interesse della cybersicurezza nazionale, al Presidente del Consiglio è riconosciuta la possibilità di utilizzare strumenti ibridi riferibili solo in parte alla tutela dell'economia (*golden powers*) su atti e operazioni suscettibili di coinvolgere la sicurezza o l'integrità delle reti e, in generale, nei settori ad alta intensità tecnologica. In tema si richiama L. Fiorentino, *Verso un sistema integrato di sicurezza: dai poteri speciali al perimetro cibernetico*, in G. Della Cananea – L. Fiorentino (a cura di), *I "poteri speciali" del Governo nei settori strategici*, Napoli, 2020, 39 ss.

[48] I soggetti inclusi, infatti, devono effettuare un'analisi del rischio sui loro *asset* ICT, anche in relazione agli effetti di un'interruzione e/o compromissione della propria attività, nonché valutazioni sulla mitigazione di questi eventi. In particolare, poi si prevede un obbligo di comunicazione al CVCN per qualsiasi fornitura di prodotti e servizi, secondo il procedimento di notifica regolato dal d.P.R. 54/2021.

La definizione delle modalità di attuazione del perimetro di sicurezza è stata demandata a successivi decreti attuativi.[49]
I profili organizzativi individuati dal d.l. 105/2019 prevedono l'istituzione, presso il Ministero dello sviluppo economico, prima, presso l'ACN, ora, del Centro di Valutazione e di Certificazione Nazionale (CVCN), con il compito di valutare e certificare le infrastrutture tecnologiche che supportano la fornitura di servizi essenziali o di funzioni essenziali per lo Stato.

5. Profili amministrativi di cybersicurezza. La creazione di nuove autorità *ad hoc* e la nuova architettura istituzionale di riferimento

Con il d.l. 82/2021, al fine di assicurare un più efficace coordinamento istituzionale, razionalizzare le competenze amministrative già delineate dal D.P.C.M. del 17 febbraio 2017 (c.d. Decreto Gentiloni) e introdurre strumenti che consentano di affrontare con efficacia e tempestività le situazioni di emergenza che coinvolgano profili di sicurezza cibernetica, è stata istituita l'Agenzia per la Cybersicurezza Nazionale-ACN[50].
Come già osservato, la cybersicurezza coinvolge una molteplicità di interessi, già oggetto di discipline puntuali ed autonome, che rendono il quadro normativo di riferimento piuttosto eterogeneo (anche in ragione delle competenze europee), stante anche l'evidente complessità tecnica della materia.[51]
Il decreto istitutivo dell'Agenzia per la Cybersicurezza Nazionale-ACN evidenza sin da subito il ruolo fondamentale[52] riconosciuto al Presidente del Consiglio dei ministri

Le misure di sicurezza, che i soggetti inclusi nel Perimetro sono tenuti ad adottare, e le modalità di notifica degli incidenti sono state definite con il D.P.C.M. 81/2021.

[49] Si fa riferimento D.P.C.M. 131/2020 per l'individuazione dei criteri sulla cui base vanno individuati i soggetti inclusi nel perimetro. In particolare, si prevede che siano le Amministrazioni competenti nei rispettivi settori strategici– interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro – ad indicare - sulla base di specifici criteri – i soggetti pubblici e privati che offrono tali servizi o funzioni essenziali. Con D.P.C.M. 81/2021, invece, si sono disciplinate le modalità e le tempistiche di notifica degli incidenti nonché ulteriori misure volte a garantire elevati livelli di sicurezza. Con D.P.C.M. del 15 giugno 2021, invece, si è proceduto all'individuazione delle categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel perimetro di sicurezza nazionale cibernetica, dai soggetti ivi inclusi. Da ultimo, si segnala il D.P.C.M. 92/2022 con cui, regolamentando l'accreditamento dei Centri di Valutazione (CV) e dei Laboratori Accreditati di Prova (LAP), sono completati i decreti attuativi necessari per supportare l'operatività dell'ACN e delle strutture che ad essa afferiscono, assicurando il presidio del perimetro di sicurezza nazionale cibernetica, sancendo l'operatività del Centro di Valutazione e Certificazione Nazionale (CVCN).

[50] Per ulteriori approfondimenti circa i profili organizzativi e funzionali dell'Agenzia si rimanda a L. Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, cit., 709-719.

[51] A tal riguardo, il Consiglio di Stato (Cons. Stato, sez. atti norm., 26 maggio 2020, n. 983) ha già manifestato la propria preoccupazione per i rischi di incoerenze e frammentarietà di un quadro normativo che, come visto, risulta piuttosto eterogeneo.

[52] Tendenza già nota in materia di sicurezza nazionale, specialmente a seguito della riforma del Sistema di informazione per la sicurezza della Repubblica *ex* l. 124/2007. In tema si veda, M. Savino, *Solo per i tuoi occhi? La riforma del sistema italiano di intelligence*, in *Giornale di Diritto Amministrativo,* 2, 2008, 121 ss.

in termini di alta direzione e responsabilità generale delle politiche di cybersicurezza e ciò tanto nei confronti dell'Agenzia (poteri di nomina, controllo e regolamentari) e, più in generale, nell'architettura istituzionale, con la previsione di ampie competenze in materia di cybersicurezza.[53]

Il decreto istitutivo, poi, affida una pluralità di funzioni all'Agenzia, sia istituendone di nuove in risposta alle necessità emerse in materia, sia redistribuendo e riaffidando alcune di quelle già previste, andando a semplificare il quadro normativo già esistente[54].

I compiti affidati all'Agenzia possono essere suddivisi in cinque macrocategorie.

La prima si riferisce alla funzione consultiva nei confronti del Presidente del Consiglio dei ministri nell'esercizio delle proprie competenze in materia di cybersicurezza ed in relazione alle iniziative legislative o regolamentari concernenti - anche solo parzialmente - la cybersicurezza, al fine di promuovere la definizione e il mantenimento di un quadro giuridico nazionale aggiornato e coerente

La seconda si riferisce alle funzioni di coordinamento interistituzionale e cooperazione internazionale (in raccordo con il Ministero degli esteri). In particolare, l'ACN garantisce l'unità dell'azione amministrativa mediante la predisposizione della strategia nazionale di cybersicurezza adottata poi dal Presidente del Consiglio dei ministri. Tra le ipotesi di collaborazione – indicate in termini generali[55] - pare interessante osservare l'espressa indicazione della possibilità di dotarsi di strumenti di coordinamento *ad hoc* con l'Autorità Garante per la protezione dei dati personali[56].

La terza si riferisce a funzioni di certificazione e qualificazione e relativi poteri ispettivi e sanzionatori. In particolare, l'Agenzia viene indicata quale autorità nazionale di certificazione della cybersicurezza ai sensi dell'art. 58 del regolamento (UE) 2019/881 con i relativi compiti di vigilanza, ispezione e sanzione.[57]

---

[53] In particolare, il Presidente del Consiglio gode rilevanti poteri nei confronti dell'Agenzia e preside il Comitato interministeriale per la cybersicurezza ed è il «vertice del Sistema di informazione per la sicurezza della Repubblica, ai fini della tutela della sicurezza nazionale anche nello spazio cibernetico» (art. 3, D.P.C.M. del 17 febbraio 2017, cit.). Ed ancora il Presidente del Consiglio ha il potere di disporre la «disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi», in caso di rischio grave e imminente per la sicurezza nazionale, ma solo «ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, secondo un criterio di proporzionalità» e previa deliberazione del Comitato interministeriale per la cybersicurezza (art. 5, d.l. 105/2019). Si devono altresì richiamare gli ulteriori poteri di controllo, collaborazione e interazione che il quadro normativo di riferimento attribuisce al Presidente del Consiglio e che sono stati qui richiamati diffusamente nel testo e nelle precedenti note. In senso critico a tale accentramento atteso il rischio di frammentarietà della disciplina è L. Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, cit., 718.

[54] Ad esempio, l'ACN assorbe le funzioni in materia cybersicurezza già proprie del Dipartimento delle informazioni per la sicurezza (DIS), del MISE e dell'AgID. Si veda la Tabella A nella quale si è cercato di riportare, senza pretesa di esaustività, l'evoluzione delle competenze in materia nel tempo.

[55] Non soltanto al fine di ottenere, nel rispetto delle diverse competenze, l'assistenza di altri organi o amministrazioni dello Stato, incluse le forze di polizia, ma altresì al fine di dare concreta attuazione ai trasferimenti delle competenze già esistenti n favore dell'Agenzia.

[56] Protocollo d'intesa stipulato in data 26 gennaio 2022.

[57] Facendo proprie le funzioni del Centro di Valutazione e di Certificazione Nazionale (CVCN), in tema di valutazione e certificazione delle infrastrutture tecnologiche che supportano la fornitura di servizi essenziali o di funzioni essenziali per lo Stato. Dal Ministero dello Sviluppo economico il CVCN è trasferito presso l'Agenzia e la sua operatività è assicurata dal 30 giugno 2022.

L'Agenzia, ancora, garantisce la qualificazione dei servizi cloud per la pubblica amministrazione e accredita, quali organismi abilitati a certificare la conformità dei sistemi di rispettiva competenza, le strutture specializzate del Ministero della difesa e del Ministero dell'interno, delegate a rilasciare il certificato europeo di sicurezza cibernetica.
La quarta si riferisce, invece, all'esercizio di poteri di vigilanza (e corrispettivi poteri sanzionatori) che vengono svolti tanto nell'ambito del perimetro di sicurezza nazionale cibernetica[58] quanto nell'ambito del proprio ruolo di Autorità nazionale competente e punto di contatto unico ai sensi della direttiva NIS in materia di sicurezza delle reti e dei sistemi informativi.
La quinta si riferisce a poteri di *moral suasion* mediante l'adozione di potere di linee guida contenenti regole tecniche di cybersicurezza nonché mediante la diffusione della consapevolezza dell'importanza della *cybersicurezza* mediante attività formative rivolte ad enti universitari, di ricerca e imprese, con i quali può concludere accordi e altre forme di partenariato pubblico-privato.
In senso trasversale all'Agenzia sono riconosciute poteri e funzioni della cd. *cyber-resilienza* quale individuazione ed attuazione delle misure necessarie a rafforzare le capacità nazionali di difesa cibernetica, attraverso il coordinamento istituzionale con gli altri soggetti pubblici coinvolti nonché mediante la promozione di iniziative dirette a sviluppare la digitalizzazione, riducendone il grado di vulnerabilità.
L'osservazione dei compiti attribuiti, anche con riferimento alla *cyber-resilienza,* rende evidente l'evoluzione rispetto alla precedente architettura istituzionale, nella quale era si riscontrava, invece, uno stretto legame tra il quadro nazionale della governance in materia di cybersicurezza e le strutture coinvolte nelle questioni di sicurezza nazionale. In realtà, nonostante le materie siano comunque affini e, spesso, orientate nella medesima direzione, il decreto istitutivo dell'Agenzia per la Cybersicurezza Nazionale separa le competenze direttamente riferibili alla sicurezza nazionale (cd. *cyberintelligence* da quelle proprie della cybersicurezza e della *cyber-resilienza* In tal senso, infatti, deve essere letto, l'accentramento di competenze in capo all'Agenzia e la conseguenziale spoliazione di competenze in capo agli organismi di informazione e sicurezza (*in primis,* CISR e DIS), pur attribuendo poteri di controllo in capo al Comitato parlamentare per la sicurezza della Repubblica (COPASIR)[59].
Come visto, allora, l'Agenzia per la Cybersicurezza Nazionale si inserisce in più ampio contesto istituzionale, adeguatamente razionalizzato mediante una generale redistribuzione delle competenze amministrative in materia – anche creandone di nuove – quanto individuando apposite sedi di coordinamento istituzionale[60]. In tal senso, dunque,

[58] Già attribuiti *ex* d.l. 105/2019 alla Presidenza del Consiglio dei ministri e al Dipartimento delle informazioni per la sicurezza.

[59] Il Presidente del Consiglio dei Ministri, infatti, è tenuto a trasmettere al Comitato parlamentare per la sicurezza della Repubblica (COPASIR) (ad ulteriore evidenza – ove vi fosse ancora qualche dubbio - della correlazione tra la *cybersicurezza* e la sicurezza nazionale), con cadenza annuale (entro il 30 giugno), una relazione sulle attività svolte nell'anno precedente dall'Agenzia negli ambiti concernenti la tutela della sicurezza nazionale nello spazio cibernetico relativamente ai profili di competenza del COPASIR. Analoga relazione viene trasmessa al Parlamento sull'attività svolta dall'Agenzia nell'anno precedente.

[60] Ad esempio, il Nucleo di sicurezza cibernetica (NSC), già incardinato presso il Dipartimento delle informazioni per la sicurezza, con funzioni di raccordo tra le diverse componenti dell'architettura istituzionale in materia, viene ora trasferito presso l'Agenzia.

si deve ricordare che il quadro istituzionale è arricchito dalla costituzione del "Nucleo per la cybersicurezza" e del "Comitato interministeriale per la cybersicurezza" con il compito di affiancare le autorità e gli organi già esistenti e già provvisti di competenze in materia di sicurezza cibernetica al fine di assicurare un più efficace coordinamento interistituzionale[61].

Il Nucleo per la cybersicurezza, in particolare, supporta il Presidente del Consiglio nella predisposizione e attivazione delle procedure di allertamento in caso di crisi cibernetiche, nonché nella prevenzione di queste ultime. Sulla base di tali attività, l'Agenzia darà attuazione ai provvedimenti assunti dal Presidente del Consiglio, controllandone anche la corretta esecuzione. Il Nucleo per la cybersicurezza ha un importante ruolo operativo in relazione alle situazioni di crisi cibernetica (tanto mediante attività di programmazione e pianificazione delle risposte da adottare, quanto mediante l'elaborazione delle procedure di coordinamento interministeriale). In occasione di minacce per la cybersicurezza valuta se tali eventi assumano intensità o natura tali da non poter essere fronteggiati adeguatamente dalle singole amministrazioni e può imporre l'adozione di decisioni coordinate in sede interministeriale, dandone tempestiva informazione al Presidente del Consiglio dei ministri.

Istituito presso la Presidenza del Consiglio dei ministri, al Comitato interministeriale per la cybersicurezza, invece, sono attribuite funzioni consultive di consulenza, bilancio, indirizzo e proposta[62] e vigilanza[63] in materia di politiche di cybersicurezza[64].

6. Conclusioni. Il prisma di Newton nella regolazione dei dati, l'esempio della *cybersicurezza*

Il presente contributo si è aperto con la descrizione del nuovo ruolo dei dati, si sono poi accennate le connesse tematiche della cybersicurezza – prendendole ad esempio - ed ora, concludendo, si vuole tracciare una linea lungo cui estendere l'ambito di indagine per ricomprendervi l'intera regolazione amministrativa dei dati, equiparandola al prisma di Newton.

L'immagine è nota ai più e riproduce il fenomeno della rifrazione: la luce bianca entra

[61] Che, come osserva L. Parona, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, cit., si tratta, in particolare, del Presidente del Consiglio dei ministri, del Comitato interministeriale per la sicurezza della Repubblica (CISR), del Dipartimento delle informazioni per la sicurezza (DIS), dell'Agenzia informazioni e sicurezza esterna (AISE), dell'Agenzia informazioni e sicurezza interna (AISI) e del Comitato parlamentare per la sicurezza della Repubblica (COPASIR). Si tratta, come già osservato, di enti posti a garanzia della sicurezza nazionale, tutti istituiti o riformati dalla l. 124/2007.

[62] In particolare, presso il Comitato interministeriale per la cybersicurezza (CIC) propone al Presidente del Consiglio gli indirizzi generali da perseguire nel quadro delle politiche di cybersicurezza e promuove l'adozione di iniziative volte a favorire la collaborazione, anche a livello internazionale, tra soggetti istituzionali e operatori privati ai fini dell'adozione delle migliori pratiche.

[63] Quanto poi alle funzioni di vigilanza, il Comitato esercita l'alta sorveglianza sull'attuazione della strategia nazionale di cybersicurezza.

[64] Al Comitato interministeriale per la *cybersicurezza*, come visto, sono affidate tutte le funzioni di consulenza e proposta già attribuite al CISR (fatta eccezione per quelle previste dall'art. 5, d.l. 105/2019, in materia di determinazioni del Presidente del Consiglio dei ministri in caso di crisi di natura cibernetica).

nel prisma, si separa nello spettro dei colori costituenti, e, nell'uscire, li manifesta e li accentua per effetto della rifrazione.
Visivamente, il prisma di Newton esplicita la tesi che si propone: l'unicità del fenomeno dell'utilizzo dei dati a fini decisionali nelle economie data driven (la luce bianca), passando attraverso la necessità, *recte* doverosità, di una regolazione pubblica (il prisma), ne esce in un fascio di competenze e attribuzioni distinte (lo spettro dei colori costituenti), che sollevano questioni interpretative che si vanno ponendo.
Le istanze di certezza del diritto in materia di regolazione dei dati sono accentuate dalla considerazione per la quale questi vengono a costituire la base per comprendere e disciplinare lo sviluppo dell'intelligenza artificiale – verso il quale ci si dirige ad ampi passi.
Il fenomeno dell'affermazione del valore economico dei dati, elaborati mediante algoritmi e sistemi di intelligenza artificiale, si deve osservare nel tradizionale rapporto tra diritto e tecnologia, che si viene ad intrecciare in un profondo legame che li rende assolutamente permeabili alle novità, l'uno dell'altro. Da una parte, infatti, il diritto è chiamato a disciplinare le nuove possibilità offerte dall'evoluzione tecnologica, dall'altra quest'ultima influenza la quotidianità dei rapporti giuridici[65] e, per quanto d'interesse, anche le modalità con cui opera la pubblica amministrazione. Infatti, se da un lato il sorgere di nuovi interessi e nuove dinamiche sociali impone una tutela e regolamentazione delle situazioni quanto attraverso la creazione di nuove forme di tutela[66]; dall'altro, allo stesso tempo, è anche il diritto ad utilizzare l'evoluzione tecnologica per il perseguimento dei propri fini[67].
La *cybersicurezza*, infatti, al pari di ogni disciplina che coinvolge l'utilizzo nei processi decisionali dei dati (anche con finalità commerciali), si scontra con più o meno inedite questioni ordinamentali che qui possono essere così indicate nell'ibridazione delle competenze (*i*) e nell'internazionalizzazione dei fenomeni da regolare (*ii*); nella necessità di acquisire maggiori competenze tecniche (*iii*) e di rapidi tempi di reazione (*iv*).
È stato già osservato come le peculiarità dell'utilizzo dei dati (anche personali) nei processi decisionali, tanto pubblici quanto privati, conducono ad un coinvolgimento di distinti interessi pubblici, la cui tutela è affidata ad altrettante autorità amministrative e disciplinata secondo distinti plessi normativi. In tal senso, ad esempio, si sta animando il dibattito circa la possibilità di individuare illeciti antitrust attuati mediante la violazione di norme poste a tutela della privacy[68] e, in termini più generali, circa la

[65] Le rivoluzioni scientifiche e tecnologiche contribuiscono a modificare i paradigmi sociali e, quindi, giuridici: portano a trasformazioni anche radicali della società umana e, conseguentemente, del contesto normativo di riferimento. Si pensi, ad esempio, alle questioni di bioetica che il progresso scientifico ha sollevato. Per un'analisi delle connessioni tra tecnologia e sviluppo economico, invece, si veda M. Clarich, *Istituzioni, nuove tecnologie, sviluppo economico*, in *Diritto pubblico,* 1, 2017, 75 ss.

[66] Il diritto è, infatti, una scienza sociale e, come tale, risente delle grandi direttrici di cambiamento della società. Il diritto mantiene una funzione ordinatrice anche riguardo ai mutamenti tecnologici e scientifici della società. Si pensi alla crescente sensibilità maturata in ambito ecologico che ha portato ad un ripensamento del diritto ambientale, ad esempio, ovvero all'impatto avuto dall'espansione dell'industria ferroviaria.

[67] È evidente, allora, che il diritto – e non solo quello amministrativo – risenta della trasformazione in essere della società contemporanea derivante dallo sviluppo dell'informatica e dell'intelligenza artificiale.

[68] È stato osservato, infatti, che il potere raggiunto venga esercitato nei confronti dei consumatori,

crescente interdisciplinarietà portata dai descritti fenomeni.[69] Ad oggi, a legislazione invariata, le amministrazioni, nel perseguimento degli interessi pubblici che sono loro affidati, sono chiamate a rispondere alle nuove sfide poste dalle economie dei dati, non soltanto nella rappresentata maggiore interdipendenza tra competenze e i rispettivi plessi amministrativi di riferimento ma altresì nella maggiore cooperazione ed interazione a livello internazionale determinata dalla rilevanza sovranazionale dei dati e della loro circolazione.

Tali questioni conducono ad una necessaria analisi della perdurante efficacia dei tradizionali istituti amministrativi e, in particolar modo, delle modalità con cui queste trovano applicazione procedimentale: ciò che si vuole sostenere è che la struttura del diritto amministrativo, ancorata saldamente su principi cardine di carattere generale,[70] non deve necessariamente essere oggetto di specifici adattamenti a fronte di mutamenti rivoluzionari che interessano la società di riferimento: ciò non significa però che il quadro normativo di riferimento sia sempre sufficiente alla regolazione dei nuovi fenomeni economici e sociali che il progresso scientifico consente.

sottoponendoli anche a processi e trattamenti in contrasto con i loro diritti fondamentali (tra tutti, la privacy, la libertà di autodeterminazione) piuttosto che in violazione delle regole proconcorrenziali. La letteratura sul tema si va ampliando e, senza pretesa di esaustività, si richiama, G. Pitruzzella, *Big data, competition and privacy: a look from the antitrust perspective,* in *Concorrenza e mercato,* 23, 2016; G. Colangelo – M. Maggiolino, *Big data, data protection and antitrust in the wake of the "bundeskartellamt" case against Facebook*, in *Rivista Italiana Antitrust*, 1, 2017, 104 ss.; M. Midiri, *Privacy e antitrust: una risposta ordinamentale ai Tech Giant*, in *Federalismi.it*, 14, 2020, 209 ss. Recente è anche M. E. Stucke, *The Relationship Between Privacy and Antitrust*, in *Notre Dame Law Review*, in corso di pubblicazione, in *ssrn.com*, 5 marzo 2022; F. Costa – C.O. Lynskey, *Family ties: the intersection between data protection and competition in EU law*, in *Common Market Law Review*, 54(1), 2017, 11 ss.

[69] In termini più generali, si veda, ad esempio, L. Tarasco – M. Giaccaglia, *Facebook è gratis? "Mercato" dei dati personali e giudice amministrativo*, in *Il diritto dell'economia,* 102, 2020, 265 ss.; S. Gobbato, *Big Data e "tutele convergenti" tra concorrenza, GDPR, e Codice del Consumo,* in questa *Rivista,* 3, 2019, 148 ss. Sul rapporto tra antitrust e tutela della proprietà intellettuale, si rimanda a M. Maggiolino – L. Zoboli, *The Intersection Between Intellectual Property and Antitrust Law*, in I. Calboli – M. L. Montagnani (a cura di), *Handbook on Intellectual Property Research*, Oxford, 2021.

[70] Cons. Stato, Ad. Plen., sent. 3/1981.