amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Rivista scientifica trimestrale di diritto amministrativo (Classe A)

Pubblicata in internet all'indirizzo www.amministrativamente.com

Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico"

Direzione scientifica
Gennaro Terracciano, Gabriella Mazzei, Julián Espartero Casado

Direttore Responsabile
Gaetano Caputi

Redazione
Giuseppe Egidio Iacovino, Carlo Rizzo

FASCICOLO N. 2/2023

Estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009
ISSN 2036-7821

Comitato scientifico

Annamaria Angiuli, Antonio Barone, Vincenzo Caputi Jambrenghi, Francesco Cardarelli, Enrico Carloni, Maria Cristina Cavallaro, Guido Clemente di San Luca, Andry Matilla Correa, Chiara Cudio, Gianfranco D'Alessio, Mariaconcetta D'Arienzo, Ambrogio De Siano, Ruggiero Dipace, Luigi Ferrara, Pierpaolo Forte, Gianluca Gardini, Biagio Giliberti, Emanuele Isidori, Bruno Mercurio, Francesco Merloni, Giuseppe Palma, Alberto Palomar Olmeda, Attilio Parisi, Luca Raffaello Perfetti, Fabio Pigozzi, Alessandra Pioggia, Helene Puliat, Francesco Rota, Josè Manuel Ruano de la Fuente, Leonardo J. Sańchez-Mesa Martĩnez, Ramón Terol Gómez, Antonio Felice Uricchio.

Comitato editoriale

Jesús Avezuela Cárcel, Giuseppe Bettoni, Sveva Bocchini Salvatore Bonfiglio, Vinicio Brigante, Sonia Caldarelli, Giovanni Cocozza, Andrea Marco Colarusso, Sergio Contessa, Manuel Delgado Iribarren, Giuseppe Doria, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Margherita Interlandi, Laura Letizia, Federica Lombardi, Gaetano Natullo, Carmen Pérez González, Giovanni Pesce, Marcin Princ, Antonio Saporito, Giuliano Taglianetti, Simona Terracciano, Salvatore Villani, Stefania Terracciano.

Coordinamento del Comitato editoriale

Valerio Sarcone.

ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Cybersecurity, sicurezza nazionale e trattamento dei dati personali

di Marta Maurino

(Assegnista di ricerca presso l'Università degli Studi della Campania *"Luigi Vanvitelli"*)

Sommario

1. Oggetto e obiettivo dello studio. – 2. Stato dell'arte. – 3. Il quadro normativo posto a tutela della protezione dei dati nello spazio cibernetico. – 4. La disciplina del trattamento dei dati nel corso delle attività di *cybersecurity* effettuate per finalità di sicurezza nazionale – 5. Il bilanciamento tra *cybersecurity*, sicurezza nazionale e diritto alla protezione dei dati personali operato dalla Corte di Giustizia dell'U.E. – 6. *Cybersecurity* e protezione dei dati personali. Profili ricostruttivi. – 7. Brevi considerazioni conclusive.

Abstract

This paper aims to investigate the balance between cybersecurity, national security and the right to the protection of personal data. Starting from the analysis of the perimeter within cybersecurity activities involving the processing of personal data for national security purposes allow limitations of the right to data protection in the cyberspace, the objective of study is to clarify how far the interest in cybernetic security justifies derogations from the general regulation about the protection of individuals with regard to the processing of personal data.

* *Il presente lavoro è stato sottoposto al preventivo referaggio secondo i parametri della double blinde peer review*

ISSN 2036-7821

1. Oggetto e obiettivi dello studio

Il presente contributo ha ad oggetto il rapporto tra diritto alla protezione dei dati personali e sicurezza cibernetica.

La portata della raccolta e della condivisione di dati personali[1] è aumentata in modo significativo in ragione dell'accelerazione nell'utilizzo delle tecnologie digitali e del fenomeno economico della globalizzazione[2].

[1] Si definisce dato personale qualsiasi 'frammento' dell'identità dell'individuo cui il dato si riferisce, definito dall'art. 4, par. 1, n. 1), GDPR come "*qualsiasi informazione riguardante una persona fisica identificata o identificabile*". Corollario di tale definizione è la collocazione della tutela del dato personale nell'alveo dei diritti della personalità e il conseguente inserimento del diritto alla protezione dei dati personali nel novero dei cc.dd. 'diritti fondamentali'. In realtà il dibattito sulla natura del diritto alla protezione dei dati personali è acceso. Parte della Dottrina ritiene che dall'inserimento di tale diritto nel novero dei diritti fondamentali nasce una evidente interferenza, declinabile nei termini che seguono: "*se (premessa maggiore) è vero che i diritti fondamentali e, tra essi in particolare, i diritti della personalità sono per definizione irrinunziabili, inalienabili e intrasmissibili; e se (premessa minore) il diritto alla tutela dei dati personali è riguardato alla stregua di un diritto fondamentale; allora (conclusione) il dato personale deve di necessità essere a sua volta partecipe di quei caratteri di irrinunziabilità, inalienabilità e intrasmissibilità*" (Cfr. B. PARENZO, *Sull'importanza del dire le cose come stanno: ovvero, sul perché della necessità di riconoscere la natura patrimoniale dei dati personali e l'esistenza di uno scambio sotteso ai c.d. servizi digitali "gratuiti"*, in *Diritto di Famiglia e delle Persone (Il)*, fasc.3/2021, pp. 1457 ss., il quale, sul punto, richiama A. DE CUPIS, *I diritti della personalità*, in *Tratt. dir. civ.* comm. Cicu-Messineo, Milano, 1982, passim; P. RESCIGNO, voce *Personalità* (diritti della), in *Enc. giur.*, XXIII, Roma, 1990, p. 7; V. ZENO-ZENCOVICH, voce *Personalità* (diritti della), in Dig. disc. priv., sez. civ., XIII, Torino, 1995, 430; G. RESTA, *Dignità, persone, mercati*, Torino, 2014, p. 73. Intendere il diritto alla protezione dati nei termini sopra descritti porterebbe ad un'unica conclusione: la non ammissibilità dei medesimi alla circolazione, non potendo gli stessi essere dedotti in contratto e/o commercializzati. Cionondimeno, la realtà socio-economica restituisce allo studioso una verità differente in grado di mettere in crisi la tradizionale ricostruzione giuridica esposta. Come osservato da parte della Dottrina, infatti, "*è solo bendandosi e chiudendosi in una stanza buia che non si vede che le più grandi [...] società al mondo sono data companies, come Google e Facebook*" (Cfr. G. RESTA e V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, p. 416). Ciò che emerge evidente è che i dati personali costituiscono la materia prima dei processi produttivi del Terzo millennio e che nelle variazioni dei mercati e nelle decisioni commerciali assunte dagli operatori economici sono sempre più determinati le analisi dei dati personali disvelati dalle navigazioni degli utenti della rete. V'è, quindi, chi sostiene che le cd. *non-monetary transactions* presentino carattere di sinallagmaticità, ossia caratteri del contratto di scambio in senso proprio: "*la prestazione di un bene o di un servizio all'interessato non è semplicemente l'occasione fattuale o una mera circostanza nella quale quello stesso interessato presta il proprio consenso al trattamento dei dati personali, ma rappresenta la ragione economica concreta dell'operazione (poiché) l'interessato presta il proprio consenso al trattamento dei dati al fine di ottenere un servizio digitale da parte dell'operatore economico (...), mentre l'operatore economico fornisce un bene/servizio digitale (...) al fine di poter sfruttare quella specifica ricchezza patrimonialmente valutabile che sono i dati personali dell'interessato*" (Cfr., in particolare, V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, p. 645). Sul medesimo tema si v., *ex multis*, V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. CUFFARO, R. D'ORAZIO e V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 25 ss.; C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali,* in *Giust. civ.*, 2019, pp. 499 ss..

[2] Sui *Big data* cfr., *ex multis*, L. ATTIAS, G. SCORZA, *La consapevolezza digitale al servizio dell'etica*, in *Diritto dell'Informazione e dell'Informatica (Il)*, fasc. 6/2019, pp. 1191 ss.; L. FLORIDI, *La quarta rivoluzione, Come l'infosfera sta trasformando il mondo*, Cortina Raffaello, Milano, 2017; T.H. DRAVENPORT e L. PRUSAK, *Working Knowledge: How Organizations Manage What They Know*, Boston, tr. It., *Il sapere al lavoro*, Etas, Milano, 2000; C. HESS e E. OSTROM, *Panoramica sui beni comuni della conoscenza*, in *La conoscenza come bene comune (Understanding Knowledge As a Commons)*, C. HESS E E. OSTROM (a cura di), MIT, 2007, ed. it. P. FERRI, BRUNO MONDADORI (a cura di),

ISSN 2036-7821

Le nuove tecnologie consentono alle imprese private e alle autorità pubbliche di utilizzare enormi quantità di dati personali nello (e per lo) svolgimento delle proprie attività come mai in precedenza.

Non tutte ma senza dubbio molte operazioni aventi ad oggetto i dati personali si svolgono nello spazio cibernetico[3], uno spazio reale, ancorché dematerializzato, creato dall'essere umano e costituito dall'insieme dei beni e servizi Ict, cioè delle componenti di rete e servizi qualificate come "*info-strutture portanti di qualsiasi organizzazione*"[4].

In tale spazio prende forma una nuova sfera privata che fa diminuire la necessità di molti consolidati e quotidiani contratti sociali, così da sottrarre il singolo individuo "*alle diverse forme di controllo sociale rese possibili proprio dall'agire 'in pubblico', in una comunità*"[5] e determina la nascita di nuove esigenze, prime tra tutte quelle legate alla sicurezza *nello* spazio e *dello* spazio cibernetico[6], condizioni necessarie all'esercizio dei diritti di libertà nello spazio digitale.

La sicurezza *nello* spazio cibernetico si sostanzia nella garanzia che il trattamento dei dati delle persone fisiche sia effettuato in modo da assicurare la sovranità delle

---

2009; C. Tabarrini, *Comprendere la "Big Mind": il GDPR sana il divario di intelligibilità uomo-macchina?*, in *Diritto dell'Informazione e dell'Informatica (Il)*, fasc.2, 1/2019, pp. 555 ss.

[3] Il lemma *cyber* origina dalla parola greca *Kyber*, "navigare". L'espressione "cyber spazio", ossia spazio cibernetico, è impiegata per descrivere uno spazio effettivamente navigabile.

[4] Si v. R. DI BIASE, *La difesa passa dalla rete*, in *AirPress, Mensile sulle politiche per l'aerospazio e la difesa*, fasc. n. 127, 2021, p. 12.

[5] Cfr. S. RODOTÀ, voce *Riservatezza*, ed. Treccani, 2021 pp. 21 ss., il quale, invitando a riflettere sul telelavoro, sulle videoconferenze, sul numero di acquisti ormai effettuati a distanza, sullo svolgimento di operazioni bancarie direttamente dalla propria abitazione, richiama quanto rappresentato in tema di tecnologie da J. E. KATZ, *Public Policy Origins of Telecommunications. Privacy and the Elarging Issues*, Information Age, 1988, p. 173, il quale evidenziava già trent'anni orsono che esse "*servono anche a mettere l'individuo al riparo da quelle forme di controllo sociale che in passato erano servite a vigilare sui suoi comportamenti e a esercitare pressioni per l'adozione di atteggiamenti di tipo conformista*".

[6] Sul tema della sicurezza nell'U.E. D. MARRANI, *Il coordinamento delle politiche per la cybersecurity dell'UE nello spazio di libertà, sicurezza e giustizia*, in *Freedom, Security & Justice: European Legal Studies*, n. 1/2021 osserva – richiamando quanto stabilito dal Consiglio dell'Unione europea, *Una strategia globale per la politica estera e di sicurezza dell'Unione europea*, Bruxelles, 28 giugno 2016, https://eeas.europa.eu/topics/eu-global-strategy_en – che "*la nozione di sicurezza dell'Unione europea quale emerge dagli orientamenti recenti, in linea con la prassi internazionale in tema di "sicurezza cooperativa" e di "sicurezza umana", è molto ampia e non coincide con il perseguimento della pace e sicurezza internazionali nell'ambito della PESC. Come è stato delineato dalla Strategia globale per politica estera e di sicurezza dell'UE nel 2016, e ribadito nei successivi orientamenti dalla Commissione europea e dall'Alto Rappresentante per gli affari esteri e la politica di sicurezza, la dimensione interna ed esterna della sicurezza sono interconnesse. Di conseguenza, la sicurezza è disciplinata in maniera unitaria negli orientamenti generali delle Istituzioni, salvo trovare attuazione in strumenti giuridici specifici per ogni diversa politica. In particolare, il nuovo approccio della Commissione europea alle crisi che riguardano la "sicurezza" è fondato sul concetto di "resilienza" trasversale a diverse politiche*". Sul punto l'A. richiama la *Comunicazione della Commissione al Parlamento europeo e al Consiglio, Relazione 2020 in materia di previsione. Previsione strategica: tracciare la rotta verso un'Europa più resiliente*, Bruxelles, 9.09.2020, COM (2020) 493 *final* e rinvia ai contributi di R. Cohen, *Cooperative Security: From Individual Security to International Stability, Marshall Center Papers*, n. 3/2001, reperibile *on-line* e L. AXWORTHY, *La sécurité humaine: la sécurité des individus dans un monde en mutation*, in *Politique étrangère*, 1999, n. 64-2, p. 337.

ISSN 2036-7821

informazioni digitali, ossia la capacità di controllarne la riservatezza, l'integrità e la disponibilità.

Nel cyberspazio, infatti, i dati che identificano i comportamenti dell'essere umano sono digitalizzati. La mancata tutela di tali dati – che definiscono l'essere umano come elettore, cittadino, lavoratore – si traduce nella impossibilità di proteggere la persona fisica con riguardo a tutti i suoi comportamenti che passano da tecnologie che li possono 'spiegare' e, addirittura, 'predire', esponendola a poteri potenzialmente incontrollabili, legati alla sorveglianza di massa, alla manipolazione politica e alla persuasione commerciale.

All'uopo, l'U.E., già con l'emanazione della Direttiva 2002/58 del Parlamento Europeo e del Consiglio del 12.07.2002 aveva inteso tutelare la vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

In tempi recenti ha poi adottato il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR)[7], fornendo un quadro normativo

[7] Con l'adozione del GDPR il Legislatore europeo ha abrogato la Direttiva 95/46/CE del Parlamento europeo e del Consiglio che aveva l'obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri, al fine di assicurare un'applicazione coerente e omogenea in tutta l'Unione delle disposizioni in tema di protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali. Come chiarito dai Considerando 9 e 10, GDPR, l'emanazione della Direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione e non ha eliminato l'incertezza giuridica o "la percezione, largamente diffusa nel pubblico", che le operazioni svolte *on-line* comportino rischi per la protezione delle persone fisiche. Con riguardo al trattamento dei dati personali, infatti, all'interno dei singoli Stati membri si è creato un divario nei livelli di protezione dovuto alle divergenze nell'attuazione e nell'applicazione la Direttiva in parola: la compresenza di diversi livelli di tutela dei diritti e delle libertà delle persone fisiche ha, infatti, costituito un ostacolo alla libera circolazione dei dati personali nel territorio dell'U.E., ponendo un freno all'esercizio delle attività economiche su scala europea, falsando la concorrenza e impedendo alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto sovranazionale. Si è, quindi, reso necessario aumentare il livello di protezione dei diritti e delle libertà con riguardo al trattamento di tali dati in modo da renderlo equivalente in tutti gli Stati membri e lo si è fatto attraverso l'emanazione di un Regolamento che detta una disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché disciplina l'esercizio del potere di controllo e assicura il rispetto delle disposizioni attraverso la previsione d un apparato sanzionatorio. Interessanti spunti di riflessione sul passaggio dalla Direttiva 95/46/CE al GDPR si rinvengono nei seguenti contributi: G. FINOCCHIARO, *Il nuovo regolamento Europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017; ID, *La protezione dei dati personali in Italia. Regolamento UE 679/2016 e D.lgs. 10 agosto 2018 numero 101,* Zanichelli, Bologna, 2019; L. BOLOGNINO, E. PELINO, C. BISTOLFI, *Il regolamento privacy europeo. Commentario alla Nuova disciplina sulla protezione dei dati personali*, Giuffrè, Milano, 2016, pp. 2 ss.; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 679/2016*, Torino, Giappichelli, 2016, pp. 43 ss.; S. SICA, V. D'ANTONIO, G.M. RICCIO, *La nuova disciplina europea della privacy,* Cedam- Wolters Kluer, Milano, 2016, pp. 5 ss.; G.M. RICCIO, G. SCORZA, E BELISARIO (a cura di), *GDPR normativa privacy. Commentario*, I ed., Wolters Kluer, Milano, 2018, pp. 3 ss. Per spunti di riflessione sulla costituzionalizzazione della privacy e sui principi della tutela dei dati personali nel GDPR si v., ex multis, G. BELLOMO, *Profili pubblicistici del data protection officer nel sistema multilivello di tutela della privacy*, Ed. Scientifica, Napoli, 2020, pp. 33 ss.

ISSN 2036-7821

più solido e coerente in tema di tutela della riservatezza e di corretto trattamento dei dati personali[8], con ciò mirando anche a creare – così come previsto dal Considerando n. 7, GDPR – il clima di fiducia necessario allo sviluppo della cd. 'economia digitale'.

Dalla sicurezza *nello* spazio cibernetico va distinta la sicurezza *dello* spazio cibernetico. Con riguardo a quest'ultima è pregnante l'esigenza di garantire che l'insieme dei beni e servizi Ict che costituiscono la struttura attraverso la quale i dati vengono trattati, non sia messo a repentaglio da attacchi informatici.

È in tale prospettiva che si sviluppa la *cybersecurity* quale "*insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche*"[9] e che rappresenta lo strumento attraverso cui le Istituzioni si assicurano la cd. 'sovranità digitale', ossia la "*capacità di una comunità di controllare il proprio destino digitale: proteggere, gestire e sfruttare i propri dati*"[10].

Indagando il perimetro entro il quale lo svolgimento delle attività di *cybersecurity* consentono limitazioni del diritto alla protezione dei dati nello spazio cibernetico, obiettivo del presente lavoro è comprendere se protezione dati e *cybersecurity* non si escludano a vicenda, ma si pongano tra loro in rapporto di complementarietà.

---

[8] Ai sensi dell'art. 4, co. 1, n. 2, Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR), per trattamento dei dati si intende "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*". Come evidenziato da M. RENNA, *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Responsabilità Civile e Previdenza*, fasc. 4/2020, p. 1343, sin dall'adozione della "*Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale*" (Convenzione di Strasburgo n. 108/1981) la normativa in tema di gestione dati ha costantemente evocato la 'sicurezza' quale principio ordinatore dell'attività di trattamento dei dati personali. Tale principio è poi stato consacrato nel GDPR all'art. 5, par. 1, lett. f). Sulla sicurezza nel trattamento dei dati si v., *ex multis*, S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973, pp. 81 ss.; Id., *Protezione dei dati e circolazione delle informazioni*, in Id., Tecnologie e diritti, Bologna, 1995, pp. 41 ss. Cfr., anche, V. FROSINI, *Diritto alla riservatezza e calcolatori elettronici*, in ALPA-BESSONE (a cura di), *Banche dati, telematica e diritti della persona*, Cedam, Padova, 1984, pp. 29 ss.; nonché, G. CORASANITI, *Esperienza giuridica e sicurezza informatica*, Giuffrè, Milano, 2003; Id., *La sicurezza dei dati personali*, in *Il Codice dei dati personali. Temi e problemi*, F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (*a cura di*), Giuffrè, Milano, 2004, pp. 111 ss..

[9] Così in art. 2, n. 1, Reg. EU 2019/881, relativo all'ENISA.

[10] Come dimostra la *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Una Strategia europea per i dati*, COM (2020) 66 final, p. 5, quello della 'sovranità digitale' è tema centrale per le politiche europee della Commissione Von der Leyen. Cionondimeno, in letteratura non sembra esservi concordia definitoria su tale concetto. Taluni evidenziano che "*nel concetto di sovranità digitale rientrano aspetti come la giurisdizione (chi la esercita sulle violazioni dei dati di un Paese ospitati in un altro?) e la tassazione (dove tassare le entrate generate dall'elaborazione dei dati?)*" (si v. R. BALDONI, *Il cyber-spazio, un dominio fin troppo umano*, in *AirPress, Mensile sulle politiche per l'aerospazio e la difesa*, fasc. n. 127, 2021, pp. 4 ss.); altri la intendono come capacità di convertire i dati generati dalle attività digitali in valore per le imprese e i cittadini ed elaborarli in conformità con le garanzie riconosciute dall'ordinamento dell'U.E. (si v. G. CAGGIANO, *Sul trasferimento internazionale dei dati personali degli utenti del Mercato unico digitale all'indomani della sentenza Schrems II della Corte di giustizia,* in *Studi sull'integrazione europea*, 2020, pp. 563 ss., spec. pp. 564-565).

ISSN 2036-7821

Onde raggiungere tale obiettivo, delineato lo stato dell'arte in tema di sicurezza cibernetica, si restituirà il quadro regolatorio posto a garanzia della protezione dei dati personali nello spazio cibernetico, individuando il perimetro applicativo della disciplina dettata dal GDPR e dal Codice in materia di protezione dei dati personali. Successivamente, attraverso lo studio della Giurisprudenza europea sul bilanciamento tra diritto alla protezione dati e soddisfazione delle esigenze di *cybersecurity*, si tenterà di comprendere se l'interesse alla sicurezza cibernetica giustifichi – e, se si, entro che limiti – deroghe alla disciplina generale dettata a tutela delle persone fisiche con riguardo al trattamento dei dati personali.

2. Stato dell'arte.

Come anticipato, la sicurezza cibernetica – ossia l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e tutti coloro che sono interessati dalle minacce informatiche[11] – è lo strumento attraverso cui le Istituzioni si assicurano la cd. 'sovranità digitale'[12].

L'utilizzo malevolo delle reti costituisce un problema per la sicurezza nello spazio di libertà, sicurezza e giustizia dell'Unione a fronte del quale si rende necessaria la cooperazione tra le autorità nazionali, di polizia e giudiziarie di tutti i Paesi membri[13].

Dalla consultazione delle Comunicazioni adottate dalla Commissione europea – *Plasmare il futuro digitale dell'Europa*, del 19.02.2020, COM (2020) 67 final.; *Il momento dell'Europa: riparare i danni e preparare il futuro per la prossima generazione*, Bruxelles, del 27.05.2020, COM (2020) 456 final. – nonché dall'approfondimento delle strategie per l'Unione della sicurezza e, segnatamente, dell'Agenda strategica del Consiglio europeo 2019-2024, emerge che l'obiettivo sovranazionale è quello di sviluppare infrastrutture 'resilienti', in grado di prevenire, dissuadere e rispondere agli attacchi alle reti, ai sistemi e ai servizi informativi, nonché utili alla costruzione di forme di cooperazione strategica a livello internazionale che favoriscano la costruzione di un ciberspazio aperto e sicuro: eventuali aggressioni, infatti, soprattutto se sferrate attraverso l'uso di *internet*, indipendentemente dal luogo di verificazione, oltre a provocare danni al singolo Stato membro, possono infatti ripercuotersi sull'economia complessiva del Mercato Unico.

Al fine di garantire un livello omogeneo di protezione dei consumatori e delle imprese nel Mercato Interno, l'U.E. ha inteso armonizzare le discipline degli Stati

[11] Per una riflessione sulla sicurezza informatica nel metaverso si v., *ex multis*, G. CASSANO, M. IASELLI, G. SPANGHER, *Cybersecurity, sicurezza nazionale e metaverso* in G. CASSANO e G. SCORZA (a cura di), *Metaverso, Diritti degli utenti – piattaforme digitali – privacy – diritto d'autore – profili penali – blockchain e NFT*, Pacini Giuridica, 2023, pp. 14 ss.

[12] In merito alla cd. 'sovranità digitale' si rinvia alla nota 11 del presente contributo.

[13] Sul punto si v. art. 67, par. 3 TFUE.

ISSN 2036-7821

membri in tema di sicurezza cibernetica, imponendo obblighi comuni agli operatori di servizi essenziali e ai fornitori di servizi digitali, adottando la Direttiva *network and information security* del 6 luglio 2016, n. 1148 (cd. Direttiva *NIS*).
La Direttiva NIS è stata attuata nell'ordinamento nazionale con l'emanazione del d. lgs. 18 maggio 2018, n. 65 (cd. Decreto *NIS*), giusta il quale l'Italia ha individuato le misure intese a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza.
L'adozione della Strategia nazionale di cybersicurezza per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale è stata demandata al Presidente del Consiglio dei ministri (cfr. art. 6, Decreto *NIS*) e, con la successiva emanazione del d.l. 14 giugno 2021, n. 82, convertito con modificazioni in l. 4 agosto 2021, n. 109, è stata definita l'architettura nazionale di cybersicurezza e istituita l'Agenzia per la cybersicurezza nazionale (ACN), cui è oggigiorno demandato l'espletamento delle attività volte a garantire la sicurezza delle reti e dei sistemi informativi.
Per lo svolgimento delle attività in parola si rende necessaria la raccolta e l'utilizzo (*rectius* il trattamento) di massicce quantità di dati (anche) personali – così come qualificati dall'art. 4, co. 1, n. 1, GDPR – mediante trasmissione degli stessi effettuata in differita ovvero in tempo reale.
Il tema della sicurezza delle reti è, dunque, profondamente connesso a quello della protezione dei dati personali.
All'uopo si osserva che la Strategia 2020 dell'U.E. in tema di sicurezza cibernetica per il decennio digitale suggerisce azioni e strumenti volti a fronteggiare le minacce informatiche che sovente derogano alle regole poste a protezione dei dati personali.
Alla luce del deperimento delle tradizionali forme di controllo sociale, al posto delle quali si impiegano controlli sempre più penetranti e globali, resi possibili dal trattamento elettronico delle informazioni[14], viene da chiedersi fino a che punto l'esigenza di garantire la sicurezza del *cyberspace* possa giustificare l'abbassamento delle tutele poste a protezione delle persone fisiche con riguardo al trattamento dei dati personali.
Gli studiosi concentratisi sul tema riconoscono i pericoli insiti nella minaccia informatica, in grado di mettere a repentaglio il funzionamento delle infrastrutture

[14] Sul punto, autorevole Dottrina ha osservato che *"la tecnologia contribuisce a far nascere una sfera privata più ricca, ma più fragile, sempre più esposta a insidie: da questo deriva la necessità di un continuo rafforzamento della protezione giuridica, di un allargamento delle frontiere del diritto alla privacy. Si può chiamare questo 'il primo paradosso della privacy': e il termine paradosso è adoperato per indicare una situazione nella quale la tensione verso la privacy entra (apparentemente) in contraddizione con sé stessa o produce conseguenze (apparentemente) inattese"* (cfr. S. RODOTÀ, voce *Riservatezza*, cit.). Sul tema si v. anche Id., *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973, pp. 81 ss.; Id., *Protezione dei dati e circolazione delle informazioni*, in Id., Tecnologie e diritti, Bologna, 1995, pp. 41 ss. Cfr., anche, V. FROSINI, *Diritto alla riservatezza e calcolatori elettronici*, in ALPA-BESSONE (a cura di), *Banche dati, telematica e diritti della persona*, Cedam, Padova, 1984, pp. 29 ss.

ISSN 2036-7821

critiche dei Paesi (ECI)[15] – e, per riflesso, la pace e la sicurezza internazionale. Ciononostante, sembrano esser concordi nel ritenere che non si possa considerare legittima 'qualsiasi' restrizione di diritti fondamentali (e, quindi, anche del diritto alla protezione dei dati personali) suffragata da esigenze di sicurezza[16].
Nella tensione che si registra tra diritti e interessi confliggenti, il presente contributo indaga i limiti all'applicazione della disciplina a tutela delle persone fisiche con riguardo al trattamento dei dati personali effettuato nello spazio cibernetico.

3. Il quadro normativo posto a tutela della protezione dei dati nello spazio cibernetico.
L'integrazione economica e sociale derivante dal funzionamento del Mercato unico ha comportato un sensibile aumento dei flussi transfrontalieri di dati personali tra operatori economici pubblici e privati.
Intendendo assicurare che, con riguardo al trattamento dei dati personali, i livelli di tutela dei diritti e delle libertà garantiti in ciascuno Stato membro non ne ostacolassero la circolazione, falsando la concorrenza[17], l'U.E. ha adottato la Direttiva n. 1995/46 del 24 ottobre 1995 con la quale ha ravvicinato le legislazioni nazionali in tema di *data protection*, stabilendo che qualsivoglia trattamento di dati personali dovesse essere eseguito lecitamente su dati adeguati, pertinenti e non eccedenti rispetto alle finalità perseguite le quali, oltre ad essere esplicite avrebbero in ogni caso dovuto essere esplicitate al momento della raccolta degli stessi[18].
L'evoluzione dei servizi di comunicazione elettronica con accesso alle reti digitali mobili a disposizione di un pubblico sempre più vasto ha posto l'esigenza di affiancare, alla disciplina dettata dalla Direttiva n. 1995/46, disposizioni

[15] Ai sensi dell'art. 2, co. 1, lett. a), Direttiva n. 2008/114 del Consiglio dell'8 dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, per 'infrastruttura critica' si intende "*un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni*". Ai sensi dell'art. 2, co. 1, lett. b), Direttiva n. 2008/114, con l'espressione 'infrastruttura critica europea' o 'ECI' si fa riferimento ad un'infrastruttura critica "*ubicata negli Stati membri il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri. La rilevanza dell'impatto è valutata in termini intersettoriali. Sono compresi gli effetti derivanti da dipendenze intersettoriali in relazione ad altri tipi di infrastrutture*". La Direttiva n. 2008/114 è stata attuata nell'ordinamento nazionale giusta decreto legislativo 11 aprile 2011 che all'art. 3, co. 1, stabilisce che "*alle informazioni sensibili relative alle IC, nonché ai dati ed alle notizie relativi al processo d'individuazione, di designazione e di protezione delle ICE, è attribuita adeguata classifica di segretezza ai sensi dell'articolo 42 della legge 3 agosto 2007, n. 124, e relative disposizioni attuative*".

[16] Cfr., *ex multis*, M. NINO, *Terrorismo internazionale, privacy e protezione dei dati personali*, Ed. Scientifica, Napoli, 2012, p. 8.

[17] Cfr. Considerando 7, Direttiva n. 1995/46.

[18] Si v. Considerando 28, Direttiva n. 1995/46.

ISSN 2036-7821

precipuamente dedicate alla tutela dei dati personali degli utenti dei servizi offerti in rete[19].

Il quadro normativo per le reti e i servizi di comunicazioni elettroniche è stato delineato a livello europeo con l'emanazione di cinque Direttive: la Direttiva n. 2002/19 del Parlamento europeo e del Consiglio, del 7.03.2002, relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate (direttiva accesso); la Direttiva n. 2002/20 del Parlamento europeo e del Consiglio, del 7.03.2002, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica e all'interconnessione delle medesime (direttiva autorizzazioni); la Direttiva n. 2002/21 del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro); la Direttiva n. 2002/22 (direttiva servizio universale); la Direttiva n. 2002/58 (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

Risale, dunque, agli albori del nuovo millennio l'adozione della Direttiva relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (è stata, quindi, adottata la Direttiva n. 2002/58 del 12 luglio 2002) le cui disposizioni, ai sensi dell'art. 1, precisavano ed integravano i contenuti della Direttiva 95/46 in tutte le ipotesi di trattamenti di dati e di comunicazioni elettroniche tramite reti e servizi pubblici.

Ai sensi del Considerando 11, analogamente a quanto stabilito dalla Direttiva n. 1995/46, la Direttiva n. 2002/58 non affrontava le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non fossero disciplinate dal diritto dell'Unione. Essa lasciava, pertanto, inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, necessari a tutelare la sicurezza

[19] Sui pregiudizi che possono derivare dai trattamenti di dati in rete si v. V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, London, 2013, pp. 150 e ss.; K. KRASNOW WATERMAN, P. J. BRUENING, *Big Data analytics: risks and responsibilities*, in Int. *Data Privacy Law*, 2014, 4, 2, pp. 89 ss.; F. BOSCO et al., *Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities*, in S. GUTWIRTH et al. (eds), *Reforming European Data Protection Law*, Springer, Dordrecht, 2015, pp. 11 ss. Sulla profilazione degli utenti definita 'schedatura sociale' cfr. S. NIGER, *Sorveglianza e nuovi diritti di libertà*, in G. FINOCCHIARO (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, in *Tratt. dir. comm. e dir. pubb. econ.*, diretto da F. GALGANO, Padova, 2008, pp. 12 ss.; V. ZENO ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Riv. dir. media*, 2018, 2, pp. 5 ss.. Sulla possibilità di controllare i comportamenti degli utenti per ottenere non solo vantaggi di tipo economico ma anche di tipo politico si v. S. PERRY, C. RODA, *Human Rights and digital technology*, London, 2017, pp. 63 ss. Con riguardo ai rischi derivanti dalla sorveglianza di massa in riferimento al controllo sociale si v, S. NIGER, *Sorveglianza e nuovi diritti di libertà*, cit., pp. 7 ss.; F. H. CATE, *Government Data Mining: The Need for a Legal Framework, Articles by Maurer Faculty*. Paper 150, 2008, pp. 477 ss.; A. MANTELERO, *Data protection, e-ticketing, and intelligent systems for public transport*, in Int. *Data Privacy Law*, 2015, V, 4, pp. 309 ss.; A. MANTELERO, G. VACIAGO, *The "Dark Side" of Big Data: Private and Public Interaction in Social Surveillance. How data collections by private entities affect governmental social control and how the EU reform on data protection responds*, in *Comp. Law Rev. Int.*, 6, 2013, pp. 161 ss.

ISSN 2036-7821

pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale.

La Direttiva in parola ha imposto agli Stati membri di garantire la sicurezza (art. 4) e la riservatezza (art. 5) delle comunicazioni effettuate tramite la rete pubblica di comunicazione, dei servizi di comunicazione elettronica accessibili al pubblico e dei relativi dati sul traffico, vietando l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni ad opera di persone diverse dagli utenti, senza consenso di questi ultimi (Considerando 7). Essa ha stabilito, altresì, che l'uso delle reti di comunicazione elettronica ai fini dell'archiviazione di informazioni o per l'accesso ad informazioni già archiviate nell'apparecchio terminale di un utente fosse consentito unicamente a condizione che lo stesso fosse stato informato in modo chiaro e completo sugli scopi del trattamento dei dati in conformità alla Direttiva 95/46 e che gli fosse stata offerta la possibilità di rifiutarlo[20].

A tal fine, oltre all'imposizione di obblighi informativi nei confronti degli utenti, è stato posto in capo ai fornitori di servizi di comunicazione elettronica accessibili al pubblico l'onere di assumere appropriate misure tecniche e organizzative, relative anche alle reti, per salvaguardare la sicurezza dei servizi offerti[21].

L'integrazione delle disposizioni della Direttiva n. 95/46 con quelle della Direttiva n. 2002/58 mirava, dunque, a far sì che, in tutto il territorio dell'Unione le persone fisiche fossero tutelate con riguardo al trattamento dei dati personali tramite comunicazioni elettroniche.

Unici limiti dei diritti e degli obblighi ivi stabiliti erano quelli previsti *ex* art. 15, Direttiva n. 2002, per la salvaguardia della sicurezza nazionale, della difesa, della sicurezza pubblica, nonché quelli posti al fine di assicurare il perseguimento dei reati[22].

Entrambe le direttive sono state attuate dal Legislatore nazionale con l'emanazione del d. lgs. n. 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali.

---

[20] Cfr. artt. 4 ss., Direttiva n. 2002/58.

[21] Con riguardo alle restrizioni all'applicazione delle disposizioni della Direttiva 2002/58, giusta il disposto dell'art.15, si prevedeva che gli Stati membri potessero adottare disposizioni legislative volte a limitare i diritti e gli obblighi fissati, qualora tali restrizioni costituissero, ai sensi dell'art. 13, par. 1, Direttiva 95/46, misure necessarie, opportune e proporzionate all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. In particolare, i diritti e gli obblighi di cui poteva essere, a determinate condizioni, prevista una limitazione erano quelli stabiliti *ex* artt. 5 e 6, *ex* art. 8, paragrafi da 1 a 4 ed *ex* art. 9, Direttiva 2002/58.

[22] Cfr. CGUE Sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, punto 71.

ISSN 2036-7821

Tale quadro normativo ha subito rilevanti innovazioni in ragione dell'esponenziale aumento dei flussi transfrontalieri di dati personali[23], cui si è accompagnata la crescente consapevolezza circa la pericolosità della minaccia cibernetica.
Ciò, da un lato, ha reso necessario intervenire sulla disciplina a tutela delle persone fisiche con riguardo al trattamento dei dati personali e, dall'altro, ha richiesto imponenti interventi normativi volti a garantire la sicurezza delle reti nelle quali i dati transitano e vengono trattati.
Sotto il primo profilo, dapprima, il Legislatore europeo è ripetutamente intervenuto sulla Direttiva n. 2002/58[24]; poi, ha abrogato la Direttiva n.95/46, adottando il GDPR nell'intento di assicurare un livello coerente ed elevato di protezione delle persone fisiche, con contestuale rimozione degli ostacoli alla circolazione dei dati personali all'interno dell'Unione[25].
Il Regolamento, con previsioni funzionali al buon funzionamento del Mercato unico[26], mira a garantire certezza del diritto e trasparenza agli operatori economici, offrendo alle persone fisiche in tutti gli Stati membri medesimi diritti azionabili; imponendo ai titolari e ai responsabili dei trattamenti stessi obblighi e responsabilità; assicurando un controllo coerente dei trattamenti dei dati con previsione di sanzioni equivalenti in tutto il territorio dell'Unione; assicurando la efficace cooperazione tra le autorità di controllo dei diversi Stati membri.
All'adozione del Regolamento, il Legislatore europeo ha stabilito che esso dev'essere applicato a tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali

[23] Si v. Considerando 6, GDPR ove si evidenzia che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano continuamente nuove sfide per la protezione dei dati personali in quanto la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia contemporanea consente, infatti, tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività.

[24] Le modifiche più rilevanti alla Direttiva 58/2002 sono intervenute con l'emanazione della Direttiva 2006/24 del 15.03.2006 del Parlamento europeo e del Consiglio aveva ad oggetto la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e con l'emanazione delle Direttiva 2009/136 del 25 novembre 2009 del Parlamento europeo e del Consiglio ha introdotto modifiche a quattro atti normativi dell'U.E. e, segnatamente, alla Direttiva 2002/22 relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica; alla Direttiva 2002/58 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e al Regolamento CE n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori.

[25] È stato osservato che la Direttiva 95/46 non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni *online* comportino rischi per la protezione delle persone fisiche. Cfr. Considerando 9, GDPR. Per una critica al modello adottato dal legislatore europeo si v. A. MANTELERO, *Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework*, in *Comp. Law & Sec. Rev.*, 2017, 33, 588 ss.

[26] Il Legislatore europeo, pur intendendo tutelare le persone fisiche con riguardo al trattamento dei dati personali, ritiene necessario che la libera circolazione dei dati all'interno dell'Unione non sia limitata né vietata da previsioni normative aventi ad oggetti il trattamento dei dati personali. Cfr. Considerando 13, GDPR.

ISSN 2036-7821

con riguardo al trattamento dei dati personali che non rientrassero in obblighi specifici previsti dalla Direttiva 2002/58[27] e, per assicurare il coordinamento e la coerenza dei due atti normativi, sottolineava la necessità di una modifica della Direttiva.

Ad oggi, dunque, l'efficace tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali tramite comunicazioni elettroniche – e, dunque, anche e soprattutto nello spazio cibernetico – passa necessariamente per il coordinamento tra i contenuti della Direttiva 2002/58 e il GDPR. Per tale ragione, l'*European Data Protection Board*, con Opinion EDPB 5/2019[28], ha chiarito che sussiste

[27] Cfr. Considerando 173, GDPR.

[28] L'art. 95 e il Considerando 173 GDPR confermano il rapporto *lex generalis-lex specialis* tra il Regolamento stesso e la Direttiva *e-privacy*. L'art. 95, infatti, prevede che il Regolamento "*non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva [e-privacy]*". Ai sensi dell'art. 1, parr. 1 e 2, della Direttiva *e-privacy*, letto alla luce dell'art. 94, par. 2, GDPR le disposizioni della Direttiva *e-privacy* "*precisano e integrano*" le disposizioni del Regolamento generale sulla protezione dei dati, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche. Tale Direttiva, infatti, ha l'obiettivo di armonizzare le "*disposizioni nazionali necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità*" (si v. art. 1, par. 1, Direttiva *e-privacy*). Pertanto, la Direttiva mira a garantire il pieno rispetto dei diritti di cui agli artt. 7 e 8 della Carta dei diritti fondamentali dell'UE. Sussiste comunque la possibilità di interazione tra la direttiva e-privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati. Con riguardo a tali ipotesi, il par. 3, punto 21, Opinion 5/2019 stabilisce che "*le questioni sottoposte al Comitato sono limitate a trattamenti che ricadono nell'ambito di applicazione materiale sia del regolamento generale sulla protezione dei dati sia della direttiva e-privacy*", in particolare, l'ambito presente parere è circoscritto a: casi in cui non esiste una interazione tra il GDPR e la Direttiva *e-privacy* perché la materia non rientra nell'ambito di applicazione del Regolamento; casi in cui non esiste una interazione tra il GDPR e la Direttiva *e-privacy* perché la materia non rientra nell'ambito di applicazione della Direttiva; casi in cui esiste una interazione tra il GDPR e la Direttiva *e-privacy* perché il trattamento ricade nell'ambito di applicazione materiale sia del GDPR sia della Direttiva. Sotto tale ultimo aspetto, la Giurisprudenza della Corte di giustizia dell'U.E. conferma che è possibile che il trattamento rientri al contempo nell'ambito di applicazione materiale della Direttiva *e-privacy* e del GDPR (si v. CGUE, Sent. 5 giugno 2018, C-210/16, ECLI:EU:C:2018:388. cfr., in particolare, i punti 33-34, nonché Conclusioni dell'avvocato generale Michal Bobek del 19 dicembre 2018, Fashion ID, C-40/17, ECLI:EU:C:2018:1039. cfr. in particolare i punti 111-115). La letteratura sul tema del *soft law* è ampia. Per un primo orientamento, si v. R.R. BAXTER, ***International Law in Her Infinite Variety, The International and Comparative Law Quarterly,*** 1980, pp. 549 ss.; O. ELIAS, C. LIM, ***General Principles of Law, Soft Law and the Identification of International Law, Netherlands Yearbook of International Law,*** 1997, pp. 3 ss. Il ***soft law*** è anche richiamato in dottrina a qualificare fenomeni giuridici diversi da quelli prodotti dagli atti tipizzati nell'ordinamento ma, comunque, produttivi di effetti giuridici negli ordinamenti nazionali. L'elemento che accomuna tale nozione di ***soft law è*** generalmente legato al diritto prodotto da organismi quali le Autorità indipendenti, ovvero organismi produttori di regole etiche, deontologiche o comportamentali. Con riferimento al primo fenomeno si v., nella dottrina nazionale, A. PREDIERI, ***L'erompere delle autorità amministrative indipendenti, Passigli,*** Firenze, 1997 e per il secondo, sempre nella dottrina italiana v. S. RODOTÀ, ***Repertorio di fine secolo, Laterza,*** Roma-Bari, 1999 pp. 13 ss.; M. LEMBO, *Gli strumenti di soft law tra l'ordinamento europeo e quello italiano*, in *Diritto del Commercio Internazionale*, fasc.4, 1° dicembre 2021, pp. 1049 ss.

ISSN 2036-7821

un rapporto di specialità tra Direttiva n. 2002/58 e GDPR in forza del quale in caso contrasto derivante dall'applicabilità ad una fattispecie di entrambe le normative, a prevalere saranno le disposizioni della Direttiva.
Con riguardo al coordinamento tra la disciplina del GDPR e quella della Direttiva n. 2002/58, il 10.01.2017 è stata presentata dalla Direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie della Commissione europea, la Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la Direttiva 2002/58 (regolamento sulla vita privata e le comunicazioni elettroniche). Cionondimeno, il coordinamento in parola non risulta, allo stato, essere (ancora) intervenuto.
Sul piano interno, ambedue le normative sono trasposte 'nel decreto legislativo 30 giugno 2003, n. 196, recante Codice in materia di protezione dei dati personali, adeguato al GDPR giusta decreto legislativo 10 agosto 2018, n. 101.
Il Codice è stato modificato nel settembre (con decreto legge 30 settembre 2021, n. 132, convertito, con modificazioni, in legge 23 novembre 2021, n. 178) e nell'ottobre 2021 (con decreto legge 8 ottobre 2021, n. 139, convertito, con modificazioni, in legge 3 dicembre 2021, n. 205) con interventi che hanno interessato il Titolo X, Capo I, artt. 121 ss., relativi ai servizi di comunicazione elettronica, ossia' al trattamento dei dati effettuato con trasmissione di segnali su reti di comunicazioni elettroniche. Sono, dunque, state parzialmente innovate le regole aventi ad oggetto il trattamento dei dati attraverso sistemi di trasmissione, apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa *internet*, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato[29] .
Tali modifiche mirano a garantire all'utente che naviga in rete l'integrità dei dati e la sicurezza dei trattamenti, attraverso l'imposizione di obblighi al fornitore del servizio di comunicazione elettronica.
Emerge, dunque, che la disciplina a tutela dell'interessato e volta e ad imporre obblighi stringenti ai titolari del trattamento, siano essi soggetti pubblici o privati, trova applicazione nello spazio reale quanto in quello cibernetico, eccetto che nei casi

[29] Cfr. art. 121, co. 1 *bis*, lett. c, d. lgs. n. 196/2003.

ISSN 2036-7821

di esclusione fissati dall'art. 2 co. 2, GDPR, nonché nelle ipotesi in cui la normativa europea riconosce agli Stati membri di limitare, con misure legislative, la portata degli obblighi e dei diritti sanciti dal GDPR e dalla Direttiva 2002/58.
Tali limitazioni devono rispettare l'essenza dei diritti e delle libertà fondamentali e risultare necessarie e proporzionate in una società democratica a salvaguardare interessi quali la sicurezza nazionale, la difesa, la sicurezza pubblica[30].
Con specifico riguardo alla gestione dei dati nel cyberspazio, un espresso limite all'applicazione delle disposizioni volte ad assicurare la protezione dei dati personali si rinviene all'art. 13, l. 109/2021, ove si stabilisce che nel corso delle attività volte a garantire la *cybersecurity*[31] i trattamenti di dati personali effettuati per finalità di 'sicurezza nazionale', devono essere eseguiti ai sensi del (solo) articolo 58, co. 2 e 3, d. lgs. n. 196/2003.
Dunque, nel corso delle attività di cybersicurezza aventi finalità di sicurezza nazionale si esclude l'applicazione delle regole contenute nel Codice in materia di protezione dei dati personali, eccezion fatta per le di disposizioni contemplate dall'art. 58, co. 2 e 3 dello stesso.
Il limite in parola richiede d'essere indagato alla luce di un chiarimento di ordine concettuale: benché, in alcune circostanze, la minaccia informatica possa costituire uno strumento per mettere in pericolo il funzionamento delle infrastrutture critiche di un Paese e pur non apparendo revocabile in dubbio che la sicurezza informatica (o cybersicurezza) possa rilevare ai fini della sicurezza nazionale e/o internazionale, la sua nozione non può essere identificata *tout court* con quella di sicurezza nazionale (e/o internazionale).
In altre parole, non tutte le minacce informatiche costituiscono un rischio per la sicurezza nazionale. La nozione stessa di cybersicurezza, infatti, è ampia e inclusiva di tutte le attività volte a garantire la sicurezza delle reti che possono rilevare anche (e non solo) sul piano della sicurezza nazionale.
La 'sicurezza nazionale', infatti, è costituita dall'insieme delle attività volte ad assicurare la protezione dello Stato-nazione da minacce che ne mettono a repentaglio l'indipendenza politica, l'integrità territoriale e la coesione socio-politica[32]. Codeste

[30] Si v. art. 23, co 1., GDPR, nonché art. 15, Direttiva 2002/58.

[31] Giusta il disposto dell'art. 1, co. 1, lett. a), l. n. 109/2021, per cybersicurezza si intende "*l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità, e garantendone altresì la resilienza*". Le attività in parola, ai sensi della l. n. 109/2021, sono state demandate all'Agenzia per la cybersicurezza nazionale (ACN), istituita con d.l. 14 giugno 2021, n. 82, convertito in l. n. 4.08.2021, n. 109, a tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico. Ai sensi dell'art. 7, Decreto *NIS*, l'ACN è designata quale autorità nazionale competente NIS per i settori e sottosettori di cui all'allegato II e per i servizi di cui all'allegato III.

[32] L'art. 4, par. 2, TUE, stabilisce che la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro. Con legge 3 agosto 2007, n. 124, l'ordinamento italiano ha innovato la disciplina del sistema di informazione per la sicurezza della Repubblica attribuendo al Presidente del Consiglio dei ministri in via

ISSN 2036-7821

attività mirano a tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società e comprendono la prevenzione e la repressione dei comportamenti – come quelli perpetrati tramite atti terroristici – che possono destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un Paese, minacciando direttamente la società e la popolazione[33].

Alla luce di tale precisazione è possibile inquadrare il limite all'applicazione della disciplina sulla protezione dei dati personali nei termini che seguono: quando le attività volte ad assicurare la sicurezza cibernetica implichino il trattamento di dati personali, il titolare del trattamento è tenuto al rispetto di tutti gli obblighi imposti dalla normativa europea e da quella nazionale a garanzia della posizione dell'interessato di cui al GDPR e alla Direttiva n. 2002/58, salvo il trattamento non sia effettuato per finalità di 'sicurezza nazionale', nel qual caso – ai sensi dell'art. 13, l. n.109/2021 – esso dovrà essere effettuato ai sensi del (solo) art. 58, co. 2 e 3, d. lgs. n. 196/2003.

Ne deriva che quella che *prima facie* parrebbe essere una rilevante limitazione dell'applicazione della disciplina a garanzia delle persone fisiche con riguardo al trattamento dei dati nel cyberspazio non riguarda tutti i trattamenti dei dati personali in ambito di *cybersecurity*, bensì solo quelli effettuati per finalità di 'sicurezza nazionale'.

La disciplina del trattamento dei dati personali effettuato per tali specifici fini è cristallizzata nell'art. 58, d. lgs. n. 196/2003 ss.mm.ii., il quale, nella sua versione originaria, imponeva che, ai trattamenti effettuati dagli organismi impegnati nei servizi per le informazioni e la sicurezza dello Stato, fossero applicate determinate disposizioni del Codice in materia di protezione dei dati (in particolare, quelle

esclusiva numerosi compiti tra i quali rientra, ai sensi dell'art. 1, co. 1, lett. a), l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza, nell'interesse e per la difesa della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento. La nozione di 'sicurezza nazionale' si distingue da quella 'sicurezza pubblica'. Come recentemente evidenziato da R. URSI, *La Sicurezza Pubblica*, Il Mulino, 2022, pp. 55 ss., pur trattandosi di ambiti strettamente correlati, essi sottendono ad interessi differenti. Mentre la sicurezza nazionale richiama una qualificazione costituzionale della sicurezza che si declina nella dicotomia istituzione - comunità e riguarda la difesa della Patria e la salvaguardia delle libere istituzioni, l'esatto inquadramento della sicurezza pubblica dipende, invece, dal differente modo di intendere i rapporti tra autorità statale e sfera individuale. Sulla sicurezza pubblica si v., *ex plurimis*, B. CARAVITA DI TORITTO, *Sicurezza e sicurezze nelle politiche regionali*, in *federalismi.it*, n. 25/2004, pp. 1-13; I. BELLONI, *Metamorfosi della sicurezza. Dall'ordine della sicurezza alla sicurezza (dell'ordine) dei diritti*, in T. GRECO (a cura di), *Dimensioni della sicurezza*, Torino, Giappichelli, pp. 75-106; E. CHITI, B.G. MATTARELLA, *La sicurezza europea*, in *Rivista trimestrale di diritto pubblico*, n- 2/2008, pp. 305-350. G. CAMPESI, *Genealogia della pubblica sicurezza*, Ombre corte, Verona, 2009, pp. 12 ss.; M. BARBERIS, *Non c'è sicurezza senza libertà*, Il Mulino, Bologna, 2017, pp. 4 ss. Sulla definizione di 'sicurezza' quale protezione della invasività proveniente da azioni esterne, di terzi stati, di organizzazioni internazionali aggressive, di organizzazioni terroristiche cfr., *ex multis*, G. De VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e dell'emergenza normalizzata*, in Rivista AIC, n. 4/2019, pp. 65-85.

[33] Cfr., *ex multis*, CGUE Sentenza 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, punto 135.

ISSN 2036-7821

previste negli artt. da 1 a 6, 11, 14, 15, 31, 33, 58, 154, 160 e 169, nonché alle disposizioni di cui agli artt. 37, 38 e 163)[34].
Dunque, anche con riguardo ai trattamenti di tale natura, l'ordinamento approntava in favore dell'interessato un'intensa tutela, prevedendo che nessun atto giudiziario o amministrativo, implicante una valutazione del comportamento umano, potesse essere fondato unicamente sul trattamento automatizzato di dati personali volto a definirne il profilo o la personalità. All'interessato veniva così riconosciuto, *ex* art. 14, co. 1 e 2, il diritto di opporsi ad ogni tipo di determinazione adottata sulla base del (solo) trattamento automatizzato.
In occasione dell'adeguamento del d. lgs. n.196/2003 al GDPR, intervenuto, come detto, ad opera del d. lgs. n. 101/2018, il Legislatore ha sottoposto l'art. 58 cit. ad una profonda modifica: abrogate le disposizioni in cui si stabiliva che i trattamenti dei dati personali eseguiti per finalità di sicurezza nazionale dovessero essere (comunque) disciplinati dal Codice in materia di protezione dati, ne ha previsto la sottoposizione al decreto legislativo 18 maggio 2018, n. 51, di attuazione nell'ordinamento nazionale della Direttiva UE n. 2016/680 del 27 aprile 2016 (cd. 'Direttiva polizia')[35].
È, dunque, alla Direttiva Polizia e al suo Decreto attuativo che dev'essere rivolta l'attenzione al fine di individuare le regole sul trattamento dei dati nelle attività di *cybersecurity* effettuate per finalità di sicurezza nazionale di cui all'art. 13, l. n. 109/2021.

4. *La disciplina del trattamento dei dati nel corso delle attività di cybersecurity effettuate per finalità di sicurezza nazionale.*
Come anticipato, l'art. 13, l. n. 109/2021, stabilisce che quando le attività di *cybersecurity* implicano trattamenti di dati svolti per finalità di sicurezza nazionale tali trattamenti devono essere effettuati ai sensi i soli commi 2 e 3 dell'art. 58, d. lgs. n. 196/2003 ss.mm.ii.
Il comma 2 dell'art. 58 cit., oltre a imporre l'applicazione degli artt. 23 e 24, d. lgs. n. 51/2018, prevede che a tutti i trattamenti effettuati per finalità di sicurezza nazionale – e, quindi, anche i trattamenti effettuati *ex* l. n. 109/2021 – si applicano le disposizioni di cui al comma 1 e, segnatamente, gli artt. 2, 3, 8, 15, 16, 18, 23, 24, 25, 37, 41, 42 e 43 del d. lgs. n. 51/2018, "in quanto compatibili".
In primo luogo, si osserva che l'uso dell'espressione "in quanto compatibili" si è reso necessario in ragione della intrinseca contraddittorietà di tale previsione: si

[34] L'art. 58, d. lgs. n. 196/2003 nella sua versione originaria è entrato in vigore il 1° gennaio 2004 e prendeva in considerazione tutti i trattamenti "*effettuati dagli organismi di cui agli articoli 3, 4 e 6 della legge 24 ottobre 1977, n. 801, ovvero sui dati coperti da segreto di Stato ai sensi dell'articolo 12 della medesima legge*" (co. 1), nonché quelli "*..effettuati da soggetti pubblici per finalità di difesa o di sicurezza dello Stato*".
[35] Cfr. art. 58, co. 1, d. lgs. n. 196/2003.

ISSN 2036-7821

richiamano le disposizioni del citato Decreto nonostante il Legislatore ne avesse espressamente escluso l'applicazione con riguardo ai trattamenti effettuati nello svolgimento di attività concernenti la sicurezza nazionale[36].

Venendo poi al contenuto delle disposizioni in esame, una prima macroscopica differenza tra la disciplina generale relativa al trattamento dei dati personali e quella in esame si rinviene nell'assenza del consenso dell'interessato quale principale base giuridica del trattamento.

Ed invero, pur prevedendo alcuni diritti in capo agli interessati[37], con la disciplina dettata dal Decreto n. 51/2018, il Legislatore ha inteso assicurare la correttezza dei trattamenti[38] solo mediante l'imposizione di obblighi ai titolari del trattamento[39]– ossia le Autorità competenti ai sensi dell'art. 2, co. 1 lett. g – nonché ai responsabili dello stesso[40].

Un elemento di rottura rispetto al passato è poi costituito dal rinnovato approccio del Legislatore europeo e, conseguentemente, di quello nazionale, rispetto ai processi decisionali automatizzati.

Sino al 2018, infatti, il Codice in materia di protezione dati, in linea con la Direttiva n. 95/46, prevedeva che nessun atto o provvedimento giudiziario/amministrativo, implicante la valutazione di un comportamento umano, potesse essere fondato unicamente su un trattamento automatizzato di dati personali attuato per definire il profilo o la personalità dell'interessato il quale poteva, ai sensi dell'art. 7, co. 4, lett. a), opporsi in ogni caso alle determinazioni adottate sulla base di trattamenti completamente automatizzati[41].

A partire dal 2016, l'U.E., giusta il disposto dell'art. 11, co. 1, Direttiva n. 680/2016, ha previsto come possibili e leciti i trattamenti completamente automatizzati, richiedendo a ciascuno Stato membro di adottare, in sede di attuazione della stessa, garanzie adeguate per i diritti e le libertà degli interessati[42].

---

[36] Il vigente art. 1, co. 3, lett. a, d. lgs. n. 51/2018, stabilisce quanto segue: "*il presente decreto non si applica ai trattamenti di dati personali: a) effettuati nello svolgimento di attività concernenti la sicurezza nazionale o rientranti nell'ambito di applicazione del titolo V, capo 2, del trattato sull'Unione europea e per tutte le attività che non rientrano nell'ambito di applicazione del diritto dell'Unione europea*".

[37] I diritti degli interessati sono trattati nel Capo II, d. lgs. n. 51/2018.

[38] Con riguardo alla modalità in cui il trattamento dev'essere effettuato, l'art. 3, d. lgs. n. 51/2018, stabilisce che qualsiasi informazione riguardante persone fisiche identificate o identificabili debba essere trattata in modo lecito (ossia per finalità determinate, espresse e legittime) e che i dati personali siano sottoposti a esami periodici che consentano di catalogarli in ragione della finalità del trattamento, in relazione alle diverse categorie di interessati previste dalla legge e distinguendo i dati fondati su fatti da quelli fondati su valutazioni con l'obiettivo di verificarne costantemente la qualità, al fine di valutare la persistenza della necessità di conservazione, ovvero la necessità di procedere alla cancellazione o anonimizzazione degli stessi.

[39] Cfr. art. 16, d. lgs. n. 51/2018.

[40] Si v. art. 18, co. 5, d. lgs. n. 51/2018.

[41] Cfr. art. 14, d. lgs. n. 196/2003, vigente sino alle modifiche introdotte giusta d. lgs. n. 101/2018.

[42] Si v. art. 11, co. 1 Direttiva n. 680/2016.

ISSN 2036-7821

Conseguentemente, il Legislatore nazionale, all'art. 8, D.Lgs. n. 51/2018, ha stabilito che, qualora il diritto dell'U.E. o specifiche disposizioni di legge le autorizzino, sono consentite le decisioni basate sul trattamento unicamente automatizzato, compresa la profilazione[43], anche qualora il trattamento riguardi categorie di dati 'particolari' *ex* art. 9, GDPR e produca effetti negativi nei confronti dell'interessato. Resta salvo, ai sensi dell'art. 8, co. 2 D.Lgs. n. 51/2018, il solo diritto riconosciuto a quest'ultimo di chiedere al titolare del trattamento l'intervento umano.

Appiattendosi sul dettato della Direttiva n. 680/2016, il Legislatore nazionale ha rinviato alle leggi di settore l'onere di adottare adeguate garanzie a tutela dell'interessato, limitandosi a stabilire, *ex* art. 25, co. 2, che in caso di trattamenti completamente automatizzati, gravi sul titolare del trattamento la responsabilità di adottare misure volte a garantire il controllo dell'accesso alle attrezzature; il controllo dei supporti di dati e dell'accesso agli stessi, nonché della loro conservazione; il controllo dell'utente; il controllo della trasmissione; il controllo dell'introduzione; il controllo del trasporto; il recupero in caso di interruzione dei sistemi utilizzati.

L'abbassamento delle tutele nei riguardi del soggetto interessato dal trattamento è tanto più evidente se si riflette su un aspetto: anche al di fuori dei trattamenti completamente automatizzati, il Capo II, d. lgs. n. 51/2018 che ha ad oggetti i diritti dell'interessato non è mai richiamato né dall'attuale art. 58, d. lgs. n. 196/2003 ss.mm.ii., né dalla l. n. 109/2021.

Si rammenta che il Capo II, all'art. 9 cit., disciplina le comunicazioni e le modalità per l'esercizio dei diritti dell'interessato; all'art. 10 elenca le informazioni da rendere disponibili o da fornire all'interessato; all'art. 11, riconosce il diritto di accesso dell'interessato; ai sensi dell'art. 12, prevede il diritto di rettifica o cancellazione di dati personali e limitazione di trattamento e, infine, *ex* art. 13, disciplina l'esercizio dei diritti dell'interessato e verifica da parte del Garante. Alcuna delle disposizioni in parola è richiamata dall'art. 13, l. n. 109/2021.

Ancora una volta, come spesso accade, esigenze di sicurezza nazionale impongono il sacrificio delle disposizioni atte a garantire le libertà e i diritti dei singoli, tra le quali senza dubbio rientrano quelle relative alla protezione dei dati personali.

Fermo restando il diritto al risarcimento del danno patrimoniale e non patrimoniale cagionato da atti e trattamenti compiuti in violazione delle disposizioni del D.Lgs. n. 51/2018 (art. 41, d. lgs. n. 51/2018) e riconosciuto all'interessato eventualmente leso *ex* art. 82 GDPR, tale evidente 'sbilanciamento' in favore della sicurezza nazionale trova nel sistema attualmente vigente, due contrappesi: l'uno, nell'azione pretoria delle Corti sovranazionali impegnate nell'individuazione dei limiti entro cui le esigenze di sicurezza nazionale possano giustificare il sacrificio delle libertà fondamentali degli

[43] L'attività di profilazione è vietata, ai sensi del co. 4, art. 8, solo se finalizzata alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali di cui all'art. 9, GDPR.

ISSN 2036-7821

individui[44]; l'altro nei poteri riconosciuti alle Autorità amministrative di controllo anche nelle ipotesi di trattamenti di cui all'art. 58, D.Lgs. n. 196/2003, in uno alla previsione di un sistema sanzionatorio volto a colpire duramente chiunque violi i principi generali relativi al trattamento dei dati personali e quelli specifici relativi ai trattamenti automatizzati.

Ai sensi dell'art. 37, D.Lgs. n. 51/2018 richiamato espressamente dall'art. 58 cit., il Garante per la Protezione dei Dati è individuato quale autorità di controllo incaricata di vigilare sull'applicazione delle norme di cui al D.Lgs. n. 51/2018, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento di dati personali e di agevolare la libera circolazione dei dati all'interno dell'Unione europea.

In quanto tale, al Garante è attribuito il potere svolgere indagini sull'applicazione del Decreto, anche in base ad informazioni ricevute da altre Autorità pubbliche; di rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento in ordine alle possibili violazioni delle norme del D.Lgs. 51/2018; di ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del Decreto, se del caso, con specifiche modalità ed entro un determinato termine, ordinando in particolare la rettifica o la cancellazione di dati personali; di imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto e il blocco dello stesso; di denunciare i reati dei quali viene a conoscenza nell'esercizio o a causa delle funzioni.

L'art. 37 riconosce, altresì, al Garante il potere di ottenere dal titolare e dal responsabile del trattamento l'accesso a tutti i dati personali oggetto del trattamento.

La disposizione in parola deve essere letta in combinato disposto con l'art. 160, D.Lgs. n. 196/2003, ove si prevede che, per i trattamenti di dati personali di cui all'art. 58, gli accertamenti relativi agli organismi di informazione e di sicurezza e ai dati coperti da segreto di Stato debbano essere effettuati per il tramite di un unico componente designato dal Garante stesso al quale, ai sensi del comma 4, è riconosciuto (solo) di poter prendere visione degli atti e dei documenti rilevanti e di riferire oralmente all'*Authority* che lo ha nominato.

In altre parole, per l'esecuzione degli accertamenti relativi agli organismi di informazione e di sicurezza oppure ai dati coperti da segreto di Stato, il controllo del Garante si sostanzia nella individuazione di un soggetto il quale potrà riferire solo in via orale degli atti di cui prenderà visione.

Come anticipato, ai poteri di controllo riconosciuti al Garante per la protezione dati si affianca la previsione di un pervasivo sistema sanzionatorio inteso a colpire il titolare del trattamento.

[44] Sul punto si rinvia al par. successivo.

ISSN 2036-7821

Il d. lgs. n. 51/2018, infatti, prevede che le violazioni delle disposizioni di cui agli artt. 3, co. 1, lett. a), b), d), e) ed f) e 8, sono punite con la sanzione amministrativa del pagamento di una somma non inferiore a 50.000,00 euro che può arrivare, nei casi più gravi, alla misura di 150.000,00 euro (art. 42, co. 3 e 4, d. lgs. n. 51/2018).
La medesima sanzione amministrativa si applica al trasferimento dei dati personali verso un Paese terzo o un'organizzazione internazionale in assenza della decisione di adeguatezza della Commissione europea. È prevista, inoltre, l'irrogazione della sanzione amministrativa del pagamento di una somma compresa tra 20.000,00 euro a 80.000,00 euro in caso di violazione della disposizione di cui all'art. 24, co 1 e 4, D.Lgs. n. 51/2018.
I controlli operati dall'Autorità indipendente preposta e il descritto sistema sanzionatorio costituiscono un deterrente contro gli abusi. Oltre ad essi, l'equilibrio protezione dei dati e sicurezza cibernetica, è costruito *case by case* dalle Corti sovranazionali e, in particolare, dalla Corte di Giustizia dell'U.E., che nel dirimere le più disparate fattispecie garantisce il bilanciamento tra diritti ed interessi apparentemente confliggenti.

5. *Il bilanciamento tra cybersecurity, sicurezza nazionale e diritto alla protezione dei dati personali operato dalla Corte di Giustizia dell'U.E.*
Come riferito, la necessità di assicurare la protezione dei dati personali e l'esigenza di garantire la sicurezza delle reti attraverso le quali tali dati transitano nascono dal considerevole aumento dei flussi transfrontalieri di informazioni personali scambiate tra attori pubblici e privati in ragione dallo sviluppo di nuove tecnologie applicate alla vita quotidiana e della implementazione del Mercato Unico.
Nel garantire la sicurezza *delle* reti, ciò che può accadere è che si prevedano deroghe ingiustificate delle disposizioni in tema di protezione dei dati personali che finiscono per tradursi in violazioni dei diritti sanciti dalla Carta dei diritti fondamentali dell'U.E. (in particolare degli artt. artt. 7 e 8) e per ingenerare effetti dissuasivi sull'utilizzo dei mezzi di comunicazione elettronica da parte degli utenti che si percepiscono violati nella propria libertà di espressione[45].
È sufficiente rammentare quanto emerso dal rapporto dell'*Intelligence and Security Committee of Parliament* che nel 2015 ha reso pubblica l'esistenza di pratiche di raccolta e di utilizzo di dati relativi a comunicazioni in massa da parte dei vari servizi di sicurezza e di *intelligence* del Regno Unito (il GCHQ, il MI5 e il MI6), o, ancora, evocare vicende quali il cd. *Datagate*, per comprendere che l'espletamento delle attività necessarie a garantire la sicurezza delle reti può facilitare la commissione di

[45] Cfr. CGUE Sent. 8 aprile 2014, *Digital Rights Ireland* e a., C-293/12 e C-594/12, EU:C:2014:238, punti 27 e 37, nonché Sent. 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punti 99 e 100 e Sent. 6.10.2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, punto 118.

ISSN 2036-7821

abusi da parte dei fornitori dei servizi di comunicazione elettronica, siano essi soggetti pubblici o privati.

L'individuazione dell'equilibrio tra diritti e interessi confliggenti deve molto alla Giurisprudenza europea e, segnatamente, all'attività pretoria della Corte di Giustizia dell'U.E. che ha concorso a delineare i limiti entro i quali le esigenze di *cybersecurity* possono giustificare ingerenze nel diritto alla riservatezza e alla protezione dei dati[46].

Tentando di districarsi tra impianti normativi europei e nazionali, le pronunce della Corte lasciano trasparire che, per quanto l'interesse alla sicurezza del cyberspazio sia pregnante, solo gravi e comprovati motivi espressamente specificati, possono giustificare l'arretramento delle tutele poste a salvaguardia del diritto fondamentale alla protezione dei dati.

In particolare, distinguendo le esigenze di sicurezza cibernetica da quelle di sicurezza nazionale, la Corte si è espressa su fattispecie eterogenee accedendo a una definizione 'elastica' di dato personale[47] e concorrendo a tracciare il perimetro entro cui esplicano i propri effetti le differenti normative di settore[48].

---

[46] Si v., *ex multis*, CGUE Sent. 16 dicembre 2008, *Heinz Huber c. Bundesrepublik Deutschland*; Id. 29 giugno 2010, C-28/08 P, Commissione europea c. *The Bavarian Lager Co.* Ltd, C-524/06. Si rammenta che il processo di rafforzamento del diritto alla protezione dei dati personali nell'U.E. ha avuto inizio nel 2014 con la pronuncia 8 aprile 2014, *Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.*, C-293/12 e C-594/12, con cui la Corte avendo constatato che la Direttiva CE n. 2006/24 non prevedeva garanzie sufficienti ad assicurare una protezione efficace dei dati conservati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, ha ritenuto che il Legislatore europeo con l'adozione della suddetta Direttiva abbia ecceduto i limiti imposti dal rispetto del principio di proporzionalità alla luce degli artt. 7, 8 e 52, par., Carta dei diritti fondamentali dell'U.E. In particolare, la Corte ha evidenziato che la Direttiva 2006/24 non prevedeva disposizioni specifiche atte a garantire gli interessati rispetto alla conservazione di vaste quantità di dati, né rispetto al rischio di accesso illecito a questi ultimi e ha posto fine alla cd. *blanket data retention*, ossia al sistema generalizzato di conservazione di massa dei dati. Sulla tutela 'forte' del diritto alla protezione dati cfr. anche CGUE Sent. 24 novembre 2011 *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL* (SABAM), C-70/10; Id. Sent. 16 febbraio 2012, C-360/10, *SABAM*; 2 Id. Sent. 4 novembre 2011, C-468 e 469/10, *ASNEF e FECEMD*; Id. Sent. 13 maggio 2014, C-131/12, *Google Spain SL e Google Inc.*; Id. Sent. 6 ottobre 2015, C-362/14, Schrems. Su tale ultima pronuncia, si richiamano le riflessioni di G. FINOCCHIARO, *La giurisprudenza della Corte di giustizia in materia di dati personali da Google Spain a Schrems*, in *Dir. inf. informatica*, 2015, p. 779 ss. e di M. NINO, *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della Corte di giustizia UE*, in *Il Diritto dell'Unione Europea*, 2016, pp. 755-787. Più in generale, sulla protezione della *privacy* e dei dati personali nella giurisprudenza della CGUE si v., *ex multis*, G. TIBERI, *La Corte di giustizia sulla conservazione dei dati: la protezione dei diritti fondamentali nel «dopo-Lisbona»*, in *Quad. cost.*, 2014, pp. 719-725; A. Oddenino, *Code is Still Law: la codificazione dei diritti in internet, la tutela dei dati personali e l'arduo contrappunto del diritto alla tecnocrazia*, in *Quaderni di SIDIBlog*, n. 2/2015, p. 279 ss..

[47] La CGUE nella Sent. 19 ottobre 2016, *Breyer* c. *Bundesrepublik Deutschland*, C-582/14, con riguardo agli indirizzi IP dinamici ha statuito che "*l'articolo 2, lettera a), della direttiva 95/46 dev'essere interpretato nel senso che un indirizzo IP dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale ai sensi di detta disposizione, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone*".

[48] Cfr., *ex multis*, CGUE Sent. 16 dicembre 2008, *Heinz Huber c. Bundesrepublik Deutschland*; Id. 29.06.2010, C-28/08 P, Commissione europea c. *The Bavarian Lager Co. Ltd*, C-524/06. Sulla tutela 'forte' del diritto alla protezione dati cfr. anche CGUE Sent. 24 novembre 2011 *Scarlet Extended SA* c. *Société belge des auteurs, compositeurs et éditeurs*

ISSN 2036-7821

Il fatto che la sicurezza cibernetica costituisca un obiettivo centrale delle politiche europee in nome del quale possono astrattamente giustificarsi ingerenze nei diritti fondamentali degli interessati è emerso chiaramente nel caso Breyer c. *Bundesrepublik Deutschland*[49], vicenda nella quale la Corte di Giustizia si è pronunciata sia sulla natura degli indirizzi IP dinamici, che sui limiti entro cui il diritto dell'U.E. – e, segnatamente, l'art. 7, lett. f), Direttiva n. 95/46 – consenta o meno a uno Stato membro di limitare il fornitore di servizi di media *on-line* nella raccolta e nell'utilizzo di dati degli utenti dei servizi offerti in mancanza del loro consenso.

La vicenda da cui è scaturito il rinvio merita, seppur in punta di penna, di essere accennata per comprendere a pieno la portata del *decisum* della Corte.

Il ricorrente proponeva un'azione inibitoria contro la Repubblica federale di Germania a causa della memorizzazione, da parte delle istituzioni pubbliche tedesche nella qualità di fornitori di servizi internet, del suo indirizzo IP.

La domanda, respinta in primo grado, è stata parzialmente accolta in appello e la Repubblica federale di Germania è stata condannata ad astenersi dal memorizzare gli indirizzi IP degli utenti oltre il termine di ciascuna operazione di accesso.

L'inibitoria era subordinata alla condizione che il ricorrente fornisse i propri dati personali nel corso dell'operazione di accesso, anche sotto forma di un indirizzo *e-mail* e che la memorizzazione non fosse necessaria al ripristino della disponibilità del servizio di telecomunicazione.

Entrambe le parti hanno poi proposto ricorso per cassazione e la VI Sezione della Corte federale di giustizia tedesca (*Bundesgerichtshof*) ha sollevato innanzi alla CGUE due questioni pregiudiziali: 1) Se l'art. 2, lett. a), Direttiva n. 1995/46 dovesse essere interpretato nel senso che un indirizzo di protocollo Internet (indirizzo IP), memorizzato da un fornitore di servizi in relazione ad un accesso al suo sito *web*, costituisse un 'dato personale' già nel momento in cui un terzo (es. un fornitore di accesso) disponesse delle informazioni aggiuntive necessarie ai fini dell'identificazione dell'utente; 2) Se l'art. 7, lett. f), Direttiva n. 1995/46 ostasse ad una disposizione di diritto nazionale in forza della quale il fornitore di servizi poteva raccogliere e utilizzare i dati personali di un utente senza il suo consenso solo in quanto ciò si rendesse necessario alla fatturazione e ad assicurare l'effettiva fruizione del servizio di telecomunicazione da parte dell'utente stesso.

In sede di rinvio, il Giudice tedesco evidenziava che – al di là degli aspetti legati alla mera fatturazione – secondo il diritto interno la conservazione dei dati personali si rendeva necessaria per garantire la sicurezza e la continuità del funzionamento dei

SCRL (SABAM), C-70/10; Id. Sent. 16 febbraio 2012, C-360/10, *SABAM*; 2 Id. Sent. 4 novembre 2011, C-468 e 469/10, *ASNEF e FECEMD*; Id. Sent. 8 aprile 2014, *Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.*, C-293/12 e C-594/12; Id. Sent. 13 maggio 2014, C-131/12, *Google Spain SL e Google Inc.*; Id. Sent. 6 ottobre 2015, C-362/14, *Schrems*.

[49] Si rinvia a CGUE Sent. 19 ottobre 2016, Breyer c. *Bundesrepublik Deutschland* (C-582/14).

ISSN 2036-7821

siti dei servizi di media *on-line* resi accessibili al pubblico, consentendo, in particolare, di riconoscere gli attacchi informatici *denial of service*, ossia gli attacchi che impediscono al fornitore di offrire i propri servizi, paralizzando il funzionamento del suo sito *web*.

Il Giudice nazionale, dunque, richiamando esigenze di sicurezza cibernetica e sostenendo che l'assunzione di misure contro gli attacchi alle reti era necessaria a rendere possibile la fruizione di media *on-line*, sottolineava che i dati presenti nei file di registro dei siti *web* dei servizi federali tedeschi – a prescindere dal consenso degli interessati – avrebbero potuto essere utili al contrasto degli attacchi cibernetici, consentendo il perseguimento penale dei 'pirati informatici'.

Al fine di individuare il perimetro applicativo della disciplina europea, la Corte di Giustizia, in linea con i propri precedenti, ha dapprima ribadito che il trattamento dei dati personali da parte dei prestatori di servizi di telecomunicazione che miri a garantire la sicurezza e il funzionamento tecnico dei suddetti servizi rientra nel campo di applicazione della Direttiva n. 95/46, restandone escluso solo quello connesso all'attività dello Stato in materia di diritto penale. Alla luce di ciò, ha evidenziato che il trattamento dei dati controversi non esulasse dall'ambito applicativo della Direttiva n. 95/46, essendo nel corso del procedimento principale emerso che la Repubblica federale di Germania aveva agito in qualità di mero fornitore di servizio *internet* e, dunque, al pari di un privato, *sine imperio*[50].

Al fine di rispondere alla prima questione pregiudiziale – ossia se un indirizzo IP potesse o meno essere considerato 'dato personale' già nel momento in cui un fornitore di accesso disponesse delle informazioni aggiuntive necessarie ai fini dell'identificazione dell'utente – la Corte, richiamando i concetti di identificabilità 'diretta' e 'indiretta', ha chiarito che per qualificare un'informazione come 'dato personale' è sufficiente che essa, messa in collegamento con altre informazioni, anche detenute da soggetti differenti (nel caso di specie il fornitore di servizi di media *online* era diverso dal fornitore di accesso a Internet), consenta l'identificazione di un utente.

In altre parole, dunque, ha ritenuto un'informazione qualificabile come 'dato personale' tutte le volte in cui, unita a dati detenuti anche da soggetti differenti, consenta di identificare l'utente.

Individuati gli indirizzi IP dinamici come 'dati personali', la Corte ha poi tracciato i limiti entro cui il diritto dell'U.E. consente a uno Stato membro di limitare la raccolta e l'utilizzo di dati degli utenti dei servizi in mancanza del loro consenso e – richiamando l'art. 7, lett. f), Direttiva n. 1995/46 – ha sancito che la normativa nazionale che consentiva la conservazione degli indirizzi IP dinamici per il solo specifico fine della fatturazione, non teneva in debita considerazione le esigenze di

[50] Cfr. punto 82, Conclusioni Avvocato Generale.

ISSN 2036-7821

cybersecurity dei servizi federali tedeschi i quali avevano necessità di garantire la continuità del funzionamento dei propri siti *web* e, richiamando un proprio precedente[51], ha rammentato che gli Stati membri potevano solo precisare le condizioni fissate dalla Direttiva 95/46 in ordine alla legittimità del trattamento, non potendo "*…introdurre, sulla base dell'articolo 5 della stessa direttiva, principi relativi alla legittimazione del trattamento dei dati personali diversi da quelli enunciati all'articolo 7 della medesima, né modificare con requisiti supplementari la portata dei sei principi previsti da detto articolo 7*".

Partendo dall'idea che una cospicua parte delle reti e dei sistemi informativi è gestita da privati o da autorità pubbliche che agiscono in qualità di privati, pur interpretando in senso ampio le disposizioni europee in tema di trattamento dei dati, la Corte ha evidenziato che la disciplina a tutela dei dati personali non può essere invocata dai Paesi membri al fine di impedire l'implementazione di sistemi atti a garantire la sicurezza cibernetica e ha riconosciuto che il diritto alla protezione dei dati personali necessita d'essere bilanciato con le esigenze di sicurezza cibernetica, finendo per far prevalere queste ultime[52].

Cosicché la Corte ha stabilito che uno Stato membro non può impedire al fornitore del servizio di media *on-line* di utilizzare i dati personali trattati anche per soddisfare esigenze di sicurezza cibernetica legate al funzionamento generale del sito *web*.

Se, da un canto, l'analisi dell'elaborazione giurisprudenziale rivela la pregnante esigenza di garantire la sicurezza cibernetica; dall'altro, non sembra potersi ritenere che la Corte attribuisca al *favor* per la *cybersecurity* un valore assoluto, riconoscendo che ingerenze ingiustificate nel diritto alla protezione dei dati possono tradursi in abusi da parte dei fornitori di servizi di comunicazione elettronica che si spesso sostanziano nell'archiviazione di informazioni e/o nell'ingiustificato accesso ed utilizzo di informazioni già archiviate.

La Corte ha, quindi, fornito ai Giudici nazionali – cui è demandata la concreta esecuzione del bilanciamento[53]– alcuni criteri-guida da applicare nell'esame delle singole fattispecie.

Tali criteri sono rinvenibili nelle disposizioni della Carta dei diritti fondamentali dell'Unione europea (in particolare, *ex* artt. 7 e 8, Carta dei diritti fondamentali dell'U.E.) e dei Trattati (Cfr. art. 16, par. 1, TFUE) e sono arricchiti dalle norme e dai principi espressi dalla Convenzione europea dei diritti dell'uomo (Conv. EDU) e

[51] Segnatamente la Sent. 24 novembre 2011, ASNEF e FECEMD, C-468/10 e C-469/10, punti 30 e 32.

[52] Cfr. anche CGUE C-582/14, cit., punto 58.

[53] Osserva D. MARRANI, *Cybersicurezza* cit., p. 816 che "*tale scelta appare giustificata in considerazione dell'applicazione del principio di sussidiarietà in base al quale è in primis il giudice nazionale (che ha sollevato la questione pregiudiziale) legittimato a conoscere dei diritti e degli interessi meritevoli di tutela nella propria comunità nazionale*". Sul bilanciamento in parola si v. *ex multis* C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Il Mulino, Bologna, 2015, pp. 163 ss.; nonché O. POLLICINO, *La «transizione» dagli atomi ai bit nel reasoning delle Corti europee*, in *Ragion Pratica*, 2015, pp. 53 ss..

ISSN 2036-7821

dalle interpretazioni della stessa fornite dalla Corte europea dei diritti dell'uomo (Corte EDU).

Le pronunce sul tema del bilanciamento tra i diritti *ex* artt. 7, 8, 10, Conv. EDU e gli altri diritti fondamentali non sono oggetto del presente saggio. Ciononostante sembra doveroso evidenziare che la Corte EDU ha delineato in via giurisprudenziale le differenze tra l'intercettazione mirata e l'intercettazione di massa e, alla luce del crescente grado di intrusione nel diritto alla *privacy* dei processi di intercettazione di massa, si è concentrata sulle cd. protezioni *end-to-end* al fine di valutare la conformità alla Convenzione del regime di sorveglianza segreta che include l'intercettazione delle comunicazioni e la condivisione di informazioni tra Paesi U.E. ed *extra* U.E.[54].

Venendo ai restanti criteri sopra elencati, dai precedenti giurisprudenziali della Corte di Giustizia emerge che le ingerenze nella sfera privata altrui attraverso il trattamento dei dati personali devono essere proporzionate e devono rispondere effettivamente a obiettivi di interesse generale riconosciuti dall'Unione, inclusa l'esigenza di proteggere i diritti e le libertà altrui.

Pur avendo censurato l'obbligo di conservazione generalizzata dei dati, la Corte non ha ritenuto del tutto inammissibili le operazioni di archiviazione per fini di sicurezza cibernetica, di sicurezza nazionale e internazionale e di ordine pubblico, enunciando una serie di criteri il rispetto dei quali consente al Paese membro di adottare disposizioni che, a titolo preventivo, consentano la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione, per finalità di lotta alla criminalità grave, a condizione che la conservazione dei dati sia limitata allo 'stretto necessario'.

In primo luogo, è necessaria la previsione di norme chiare e precise che indichino in quali circostanze e a quali condizioni una misura di conservazione dei dati può, a titolo preventivo, essere adottata. Deve, quindi, essere disciplinata la portata applicativa delle misure di conservazione dei dati, fissando i requisiti minimi per le operazioni di archiviazione, in modo che le persone i cui dati sono conservati dispongano di garanzie sufficienti a consentirne la efficace protezione contro i rischi di abuso[55].

La Giurisprudenza, inoltre, indica anche la condizione sostanziale che deve essere soddisfatta da una normativa nazionale che, nel contesto della lotta contro la criminalità, imponga o preveda la conservazione, a titolo preventivo, dei dati relativi al traffico e dei dati relativi all'ubicazione: deve essere sempre individuabile il rapporto tra i dati da conservare e l'obiettivo che si persegue, di modo che la conservazione dei dati risponda sempre a criteri oggettivi.

---

[54] Cfr. ECHR 25 maggio 2021, *Case Of Big Brother Watch And Others v. The United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15.

[55] Cfr. Sent. *Digital Rights*, cit. punto 54, nonché Sent. *Tele2 Sverige AB* c. *Post- och telestyrelsen e Secretary of State for the Home Department* cit., punti 110 - 112.

ISSN 2036-7821

Siffatte condizioni devono risultare idonee a delimitare effettivamente la portata del trattamento e limitare il pubblico interessato dalla misura della archiviazione dei dati. La Giurisprudenza ritiene che la normativa nazionale debba essere fondata su elementi oggettivi, che permettano di considerare un pubblico i cui dati sono idonei a rivelare una connessione, almeno indiretta, con atti di criminalità grave. La delimitazione in parola può essere ottenuta anche mediante un 'criterio geografico', qualora le autorità nazionali ritengano che esiste, in una o più aree, un rischio elevato di preparazione o di commissione di reati.

La Corte evidenzia, altresì: a) che l'accesso delle autorità nazionali competenti ai dati conservati deve essere subordinato, in linea di principio, salvo casi di urgenza debitamente giustificati, ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente e che la decisione di tale giudice o di tale entità intervenga a seguito di una richiesta motivata delle autorità suddette presentata, in particolare, nell'ambito di procedure di prevenzione, di accertamento o di esercizio dell'azione penale[56]; b) che le autorità nazionali competenti alle quali è stato consentito l'accesso ai dati conservati ne diano notizia alle persone interessate, nell'ambito delle procedure nazionali applicabili, a partire dal momento in cui tale comunicazione non è suscettibile di compromettere le indagini condotte dalle autorità summenzionate[57].

La tutela del diritto fondamentale al rispetto della vita privata richiede, dunque, che le deroghe alle disposizioni dettate in tema di protezione dei dati personali debbano operare entro limiti chiari e precisi atti a soddisfare il principio di proporzionalità[58]. E ciò anche qualora le restrizioni in parola siano necessarie per soddisfare obiettivi reputati 'primari' tra i quali rientra quello di salvaguardare la sicurezza nazionale quale interesse teso a tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società che comprende la prevenzione e la repressione di attività che possono destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese e, in particolare, minacciare direttamente la società, la popolazione o lo Stato in quanto tale, come specialmente le attività terroristiche[59].

---

[56] Cfr. punto 120, Sent. *Tele2 Sverige AB* c. *Post-och telestyrelsen e Secretary of State for the Home Department* cit. che sul punto richiama, per analogia, Corte EDU, Sent. 12 gennaio 2016, Szabó e Vissy c. Ungheria, parr. 77 e 80.

[57] Si v., per analogia, CGUE Sent. 7 maggio 2009, Rijkeboer, C-553/07, punto 52, nonché Id. Sent. 6 ottobre 2015, Schrems, C-362/14, punto 95.

[58] Si richiamano, *ex multis*, CGUE Sent. 16 dicembre 2008, Satakunnan Markkinapörssi e Satamedia, C-73/07, punto 56; Id. Sent. 9 novembre 2010, Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, punti 76, 77 e 86; Id. Sent. 8 aprile 2014, Digital Rights Ireland e a., C-293/12 e C-594/12, punti 52, 54 e 55; Id. Sent. 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 117; Parere 1/15 (Accordo PNR UE-Canada) 26 luglio 2017, EU:C:2017:592, punti 140 e 141.

[59] Si v.. CGUE Sent. 6 ottobre 2020 La Quadrature du Net e a., C-511/18, C-512/18 eC-520/18, punto 135.

ISSN 2036-7821

Il requisito della proporzionalità nella conservazione dei dati si ritiene soddisfatto quando una normativa preveda regole puntuali che disciplinino la portata e l'applicazione della misura limitativa e imponga requisiti che consentano alle persone i cui dati personali sono trattati di disporre di garanzie volte a proteggere efficacemente tali dati dal rischio di abusi.
Sul punto la Corte richiede che, soprattutto per le ipotesi di trattamenti automatizzati, la normativa dello Stato membro che impone trattamenti di massicce quantità di dati personali, non solo debba essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale, ma debba anche indicare in modo specifico a quali condizioni e in quali circostanze tali trattamenti possano essere effettuati.
A tale ultimo proposito, la Corte di giustizia ha ribadito che, ai sensi dell'art. 15, par.1, Direttiva 2002/58, gli Stati membri possono adottare misure derogatorie del principio della riservatezza delle comunicazioni e dei dati relativi al traffico correlati a queste ultime solo se esse si rivelano necessarie, opportune e proporzionate.
Tale orientamento è stato recentemente confermato anche con riguardo ai trattamenti di dati personali occasionati dallo svolgimento di attività cibernetiche eseguite per finalità di sicurezza nazionale.
La Corte si è espressa sulla compatibilità con il diritto dell'U.E. – e, segnatamente, con gli artt. 1 e 15, par. 1, Direttiva n. 2002/58 (direttiva relativa alla vita privata e alle comunicazioni elettroniche, come modificata dalla direttiva 2009/136 del 25 novembre 2009) – dell'obbligo generalizzato di conservazione dei dati relativi al traffico delle persone fisiche imposto da uno Stato membro ad un fornitore di servizi di comunicazione elettronica, in funzione dell'obiettivo della lotta alla criminalità, senza previsione di distinzione, limitazione o eccezione alcuna[60].
Partendo da una valutazione in ordine alla possibilità per i servizi di sicurezza e di *intelligence* nazionale di utilizzare *bulk personal data* – ossia aggregati di dati riguardanti soggetti privati quali dati biografici, dati relativi a viaggi, informazioni di natura finanziaria o commerciale, dati relativi a comunicazioni e atti a contenere informazioni sensibili, coperte da segreto professionale – raccolti nell'esecuzione delle proprie attività in forza di ordini ministeriali motivati da esigenze di sicurezza nazionale e rivolti ai fornitori di servizi di comunicazione elettronica, la Corte si è pronunciata sull'adozione di misure che, in nome della salvaguardia della sicurezza nazionale, comportano penetranti ingerenze nei diritti fondamentali.
Al fine di comprendere le ragioni poste alla base delle decisioni della Corte, è opportuno riflettere su un aspetto fondamentale relativo al transito delle informazioni attraverso le reti: i dati relativi al traffico consentono di ritrovare e

[60] Si rinvia a Corte di Giustizia Grande Sezione 6 ottobre 2020, Causa C-623/17, *Privacy International* contro *Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service.*

ISSN 2036-7821

identificare la fonte di una comunicazione e la destinazione di quest'ultima, di stabilire la data, l'ora, la durata e il tipo di una comunicazione, nonché il materiale di comunicazione degli utenti e di localizzare il materiale di comunicazione mobile. Nel novero di tali dati figurano, in particolare, il nome e l'indirizzo dell'utente, il numero di telefono del chiamante e il numero chiamato, nonché un indirizzo IP per i servizi *Internet*. Tali dati permettono di individuare la persona con la quale un utente comunica e di stabilire il tempo della comunicazione, nonché il luogo a partire dal quale quest'ultima ha avuto luogo. Insomma, presi nel loro insieme, i dati in parola sono idonei a consentire di trarre conclusioni molto precise riguardo alla vita privata delle persone e consentono di tracciare il profilo delle persone interessate dal trattamento.

È alla luce di tale premessa concettuale che si sviluppa il ragionamento della Corte di Giustizia.

Tutti i governi intervenuti nel procedimento, oltre alla Commissione, hanno osservato unanimemente che una conservazione parziale e diversificata dei dati personali, al di là delle sue difficoltà tecniche, avrebbe privato i servizi di *intelligence* nazionale della possibilità di accedere ad informazioni indispensabili per l'identificazione di minacce alla sicurezza pubblica e la difesa dello Stato, nonché per il perseguimento degli autori di attentati terroristici[61].

Da tale orientamento si è discostato dapprima l'Avvocato Generale nelle proprie Conclusioni e poi la Corte stessa evidenziando che, "*l'efficacia del potere pubblico […] trova una barriera insuperabile nei diritti fondamentali dei cittadini*", in quanto, dotando il potere pubblico di strumenti esorbitanti per il perseguimento dei reati, mediante i quali esso possa ignorare o svuotare di contenuto i diritti fondamentali, niente potrebbe assicurare che la sua azione incontrollata non si risolva in un pregiudizio alla libertà di tutti. Abbandonandosi alla mera efficacia, lo Stato di diritto perderebbe la qualità che lo contraddistingue e potrebbe diventare esso stesso, in casi estremi, una minaccia per il cittadino.

La difficoltà della lotta al terrorismo risiederebbe, dunque, proprio nel fatto che essa non dev'essere impostata pensando solo alla sua efficacia, in quanto i suoi mezzi e i suoi metodi devono rispettare i requisiti dello Stato di diritto, garantendo, anzitutto, l'assoggettamento del potere e della forza ai limiti del diritto.

[61] Dalle osservazioni presentate dai governi ceco, estone e irlandese nonché dai governi francese, cipriota, ungherese, polacco e svedese emerge che essi erano tutti sostanzialmente contrari all'applicazione della Direttiva n. 2002/58 nei confronti di una normativa nazionale avente come finalità la salvaguardia della sicurezza nazionale in quanto le attività dei servizi di sicurezza e di *intelligence* si sarebbero dovute considerare rientranti nelle funzioni essenziali degli Stati membri di esclusiva competenza di questi ultimi, come previsto dall'art. 4, par. 2, terza frase, TUE, dall'art. 1, par. 3, Direttiva n. 2002/58 nonché dall'art. 3, par. 2, primo trattino, Direttiva n. 1995/46.

ISSN 2036-7821

Orbene, nonostante forti opinioni contrarie, pur riconoscendo che l'art. 1, par. 3, Direttiva n. 2002/58, esclude dall'ambito della propria applicazione le attività dello Stato eseguite per fini di sicurezza nazionale, la Corte dapprima ha evidenziato che la Direttiva n. 2002/58 lascia inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di assumere i provvedimenti necessari a tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato e a garantire l'applicazione della legge penale[62]; successivamente ha tracciato il perimetro applicativo della Direttiva citata con riferimento ai trasferimenti di dati da parte di fornitori di servizi di comunicazioni elettroniche alle Autorità pubbliche, partendo da due assunti: a) la Direttiva deve essere considerata come disciplinante le attività dei fornitori di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nell'U.E., comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati; b) l'art. 15, par. 1, della medesima Direttiva autorizza gli Stati membri ad adottare "disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della [citata] direttiva" solo nel rispetto delle condizioni da essa previste.

La Corte ha quindi richiamato gli artt. 3 e 15, cit. e ha stabilito che rientrano nell'ambito di applicazione della Direttiva non solo le misure legislative che impongono ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi al traffico e all'ubicazione dell'utente, ma anche quelle volte ad imporre ai fornitori del servizio di accordare alle autorità nazionali l'accesso a tali dati.

Sancita l'applicabilità della Direttiva n. 2002/58 alla fattispecie sottopostale, la Giurisprudenza si è concentrata sul limite che incontra l'autorità pubblica nazionale nel richiedere ai fornitori di servizi di comunicazione elettronica la trasmissione generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione per finalità di sicurezza nazionale.

Per un verso, la Corte ha evidenziato che il divieto di intercettare le comunicazioni e i dati ad esse relativi, fissato dall'art. 5, par. 1, Direttiva n. 2002/58, ricomprende qualsiasi forma di 'messa a disposizione' dei dati oggetto di traffico in rete in favore delle autorità pubbliche. La disposizione in parola, infatti, è volta a concretizzare i diritti sanciti agli artt. 7 e 8 della Carta e fa sì che gli utenti dei mezzi di comunicazione elettronica, in linea di principio, possano fare affidamento sul fatto che le loro comunicazioni restino, senza il loro consenso, anonime, non potendo formare oggetto di registrazione.

Per altro verso, la Corte ha ribadito che l'art. 15, par. 1, Direttiva n. 2002/58 consente agli Stati membri di introdurre eccezioni all'obbligo di garantire la protezione dei

[62] Cfr. CGUE Sent. 6 novembre 2003, Lindqvist, C-101/01, punto 43, nonché Sent. 16 dicembre 2008, Satakunnan Markkinapörssi e Satamedia, C-73/07, punto 41.

ISSN 2036-7821

dati personali sancito ex art. 5, par. 1 cit., nonché agli obblighi di cui agli artt. 6 e 9 della medesima Direttiva, a patto che tale limitazione costituisca una misura 'necessaria, opportuna e proporzionata' per la salvaguardia della sicurezza nazionale, della difesa, della sicurezza pubblica o per garantire la prevenzione, la ricerca, l'accertamento e il perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica.

Pur se dalle proprie pronunce più datate emergeva che il trasferimento di dati personali da parte di imprese private ad autorità statali a fini di prevenzione e di lotta al terrorismo e ad altri reati gravi rientrava nell'ambito dei trattamenti attinenti alla pubblica sicurezza[63], la Corte di Giustizia ha reputato necessario distinguere, in relazione all'autore del trattamento dei dati, i tipi di attività rientranti nel perimetro applicativo della Direttiva n. 2002/58.

Da un canto, la Corte ha evidenziato che tale Direttiva autorizza espressamente gli Stati membri ad adottare le misure limitative in parola solo ed unicamente quando esse si rendano necessarie, opportune e proporzionate all'interno di una società democratica a salvaguardare la sicurezza nazionale, la difesa, la sicurezza pubblica e/o a garantire la prevenzione, la ricerca, l'accertamento e il perseguimento dei reati; dall'altro ha ritenuto non equiparabile la posizione di un fornitore di servizi di comunicazione elettronica a quella di una pubblica autorità.

Di talché, la Corte ha statuito che quando gli Stati membri adottano direttamente misure che derogano alla riservatezza delle comunicazioni elettroniche, senza imporre obblighi di trattamento ai fornitori di servizi di tali comunicazioni, la tutela dei dati delle persone interessate rientra non già nell'ambito di applicazione della Direttiva n. 2002/58, ma in quello del solo diritto nazionale, fatta salva l'applicazione della Direttiva n. 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU 2016, L 119, pag. 89), cosicché le misure di cui trattasi debbono rispettare in particolare il diritto nazionale di rango costituzionale e le disposizioni della CEDU.

L'imposizione di un obbligo di conservazione generalizzata non richiede, quale proprio presupposto, alcuna correlazione tra i dati di cui si chiede la conservazione e una minaccia per la sicurezza cibernetica.

[63] Cfr. CGUE Sent. 30 maggio 2006, Parlamento/Consiglio e Commissione (C-317/04 e C-318/04, EU:C:2006:346, punti da 56 a 59).

ISSN 2036-7821

Osserva la Giurisprudenza che tale obbligo non limita la conservazione nel tempo né ai dati relativi a una zona geografica determinata e/o ad una cerchia di persone suscettibili di essere implicate in una violazione grave.
Una normativa nazionale che riguarda in maniera generalizzata tutti gli abbonati e gli utenti iscritti ad un servizio di comunicazione elettronica e ha ad oggetto tutti i mezzi di comunicazione nonché l'insieme dei dati relativi al traffico, finisce per essere applicata anche a persone a carico delle quali non esiste alcun indizio e che, quindi, non si trovano neanche indirettamente in situazioni suscettibili di dar luogo ad azioni penali.
Di talché, l'imposizione, da parte di un'autorità pubblica nazionale, di un obbligo di conservazione generalizzata dei metadati oggetto delle comunicazioni elettroniche – ancorché finalizzata a contrastare il terrorismo cibernetico o la criminalità organizzata – non è stata considerata compatibile con il diritto dell'Unione in ragione della grave ingerenza nel diritto alla protezione dati che ne discende. La Corte, in particolare, ha dichiarato che una misura nazionale che preveda un obbligo generalizzato di conservazione dei dati relativi al traffico delle persone fisiche inteso ad assicurare l'efficacia della lotta alla criminalità, non può considerarsi esclusa dall'ambito di applicazione della Direttiva n. 2002/58 salvo voler privare quest'ultima di qualsiasi effetto utile e, conseguentemente, ha dichiarato l'incompatibilità della misura nazionale su citata con l'art. 15, par. 1, Direttiva n. 2002/58, letto alla luce degli artt. 7, 8 e 52, par. 1, Carta dei diritti fondamentali dell'Unione europea[64].
Dopo aver affrontato il tema dell'utilizzo di tecniche di raccolta non mirate che si basano sull'aggregazione di dati di comunicazione in un unico luogo (la cui principale utilità sarebbe stata quella di consentire l'individuazione e l'elaborazione tempestiva di obiettivi, 'qualora necessario'), la Corte ha bilanciato l'interesse all'utilizzo dei dati nell'esecuzione di attività cibernetiche volte a garantire la sicurezza nazionale (sostanziantesi nel rilevare minacce alla sicurezza nazionale 'precedentemente ignote') con il diritto alla protezione dei dati personali dei soggetti interessati dai trattamenti e ha fatto prevalere quest'ultimo.
Ancora una volta, dunque, il bilanciamento tra il diritto alla protezione dei dati e gli altri diritti e interessi presenti nell'ordinamento si risolve alla luce del principio di proporzionalità.
Per il vero, la Corte riconosce che l'obiettivo di salvaguardia della sicurezza nazionale sia nello spazio reale che in quello cibernetico può, giusta il disposto dell'art. 4, par. 2, TUE, a dir così 'superare' gli altri obiettivi previsti dall'art. 15, par. 1, Direttiva n. 2002/58, di salvaguardia della sicurezza pubblica, nonché di lotta alla criminalità in generale, anche grave. Ciò in quanto, le minacce alla sicurezza

[64] Si v. punto 103, Sent. Tele2 Sverige AB c. Post- och telestyrelsen e Secretary of State for the Home Department cit.; Cfr. Sent. 6 ottobre 2020, Causa C-623/17, *Privacy International* cit.

ISSN 2036-7821

nazionale – ossia in grado di mettere in crisi le funzioni essenziali dello Stato e gli interessi fondamentali della società – possono destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un Paese.
Dunque, fatto salvo il rispetto delle altre condizioni previste *ex* art. 52, par. 1 della Carta, l'obiettivo di salvaguardare la sicurezza nazionale può giustificare misure che comportano penetranti ingerenze nei diritti fondamentali.
Pur tuttavia, la Corte rileva che, per rispondere all'obbligo di proporzionalità, le misure che implicano il trattamento dei dati debbano essere eseguite nel rispetto delle condizioni sostanziali e procedurali fissate normativamente dallo Stato membro. In altre parole, per evitare che la sicurezza nazionale venga utilizzata per giustificare la disapplicazione delle disposizioni poste a protezione dei dati personali, l'autorità pubblica non può limitarsi ad indicare la finalità del trattamento, ma deve eseguire i trattamenti nel rispetto delle condizioni fissate dallo Stato.
Ritenendo che l'accesso 'generale' a tutti i dati conservati effettuato in mancanza di qualunque nesso, anche indiretto, con la finalità perseguita, non possa essere considerato limitato allo 'stretto necessario', la Corte – pur riconoscendo come 'astrattamente prevalente' l'obiettivo di garantire la sicurezza nazionale – si è conformata al proprio precedente orientamento in forza del quale una normativa nazionale che disciplina l'accesso ai dati relativi al traffico e ai dati relativi all'ubicazione degli interessati deve necessariamente fondarsi su criteri oggettivi che indichino le circostanze e le condizioni per il riconoscimento dell'accesso ai dati.
Dunque, anche i trattamenti effettuati per finalità di sicurezza nazionale – per quanto pregante sia la suddetta finalità – non possono essere effettuati in modo indiscriminato, gli stessi soggiacendo comunque a dei limiti.
In definitiva, sembra potersi convintamente sostenere che l'equilibrio tra protezione dati e sicurezza cibernetica debba molto alla Giurisprudenza europea. Per altro verso, concentrando l'attenzione sui trattamenti effettuati in ambito di sicurezza cibernetica per finalità di sicurezza nazionale, non v'ha dubbio che il continuo potenziamento pretorio delle garanzie a tutela degli interessati fa sì che, anche quando sussistono esigenze pregnanti, il fine di garantire la sicurezza nazionale, ossia l'indicazione della sola finalità in ragione della quale determinati trattamenti vengono eseguiti, non è da solo sufficiente a legittimare gravi ingerenze nella sfera privata dei consociati.

6. Cybersecurity e protezione dei dati personali. Profili ricostruttivi.
Come anticipato nell'introduzione al presente studio, l'utilizzo delle tecnologie digitali ha reso possibile che soggetti pubblici e privati trattino costantemente grandi quantità di dati personali, sfruttando comunicazioni elettroniche e reti nell'espletamento delle proprie attività. Ciò ha determinato la necessità di adottare –

ISSN 2036-7821

dapprima con Direttiva e, poi, con Regolamento – un impianto normativo teso a garantire la protezione delle persone fisiche con riguardo al trattamento dei dati personali (cd. protezione dei dati personali).
L'utilizzo delle tecnologie digitali ha, altresì, provocato l'esponenziale aumento delle minacce cibernetiche. Per reazione alle stesse, l'U.E. ha adottato una strategia comune a tutti i Paesi membri in tema di cybersicurezza che ha condotto alla emanazione della Direttiva Network and Information Security 2016/1148/UE (Direttiva NIS), trasposta nell'ordinamento interno giusta d. lgs. n. 65/2018 (Decreto NIS), cui è seguita l'emanazione del d.l. n. 82/2021, conv. in l. n. 109/2021, istitutivo dell'ACN.
Le discipline in parola si incontrano tutte le volte in cui il trattamento dei dati personali avviene nello spazio cibernetico e finiscono per confliggere ogni qualvolta le attività tese a garantire la sicurezza delle reti implichino il trattamento di dati personali.
Ciò può avvenire tanto nel caso in cui le attività di cybersicurezza per le quali si rende necessario il trattamento dei suddetti dati non siano espletate per finalità di sicurezza nazionale, quanto nel caso in cui lo siano.
Nel primo caso il trattamento dei dati personali da parte dei soggetti impegnati a garantire la sicurezza delle reti deve essere effettuato ai sensi del GDPR e delle disposizioni del d. lgs. n. 196/2003 ss.mm.ii.; nel secondo caso, invece, ossia quando le attività di cybersicurezza sono svolte per finalità di sicurezza nazionale, l'art. 13, l. n. 109/2021 prevede che i trattamenti di dati personali debbano essere effettuati ai sensi del (solo) art. 58, co. 2 e 3, d. lgs. n. 196/2003 ss.mm.ii. Tale disposizione, a propria volta, stabilisce che i trattamenti finalizzati a garantire la sicurezza dello Stato non debbano più essere eseguiti ai sensi di specifiche disposizioni del Codice in materia di protezione dei dati personali, bensì debbano essere effettuati ai sensi del d. lgs. n. 51/2018, relativo al trattamento in corso di attività di prevenzione, indagine, accertamento e perseguimento di reati e che, è di facile intuizione, prevede garanzie inferiori a tutela delle persone fisiche rispetto al GDPR: la soddisfazione di esigenze di sicurezza nazionale impone il sacrificio di parte delle disposizioni atte a garantire le libertà e i diritti dei singoli.
La costante tensione tra diritti ed interessi contrapposti richiede l'individuazione di un equilibrio che emerge, prevalentemente, grazie all'attività pretoria delle Corti sovranazionali ed, in particolare, della Corte di Giustizia la quale, pur intendendo soddisfare l'interesse alla stabilità delle reti e alla continuità dei servizi telematici erogati nel Mercato unico, considera legittime le limitazioni della disciplina posta a protezione dei dati personali e della riservatezza al rispetto di determinate condizioni.

ISSN 2036-7821

La Corte, in altre parole, non nega in radice la possibilità che la disciplina posta a protezione dei dati personali receda a fronte della necessità di espletare attività di *cybersecurity*, ma fissa in via interpretativa dei criteri atti ad arginare l'effettuazione, da parte degli Stati membri, di trattamenti in modo generalizzato e indifferenziato, così trasformando in regola la deroga all'obbligo di garantire la protezione dei dati personali.
Riconoscendo che i diritti sanciti agli artt. 7, 8 e 11 della Carta non sono assoluti la Corte ammette limitazioni al loro esercizio, purché le stesse siano previste dalla legge, rispettino il contenuto essenziale di detti diritti, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'U.E. o all'esigenza di proteggere i diritti e le libertà altrui.
In via interpretativa, dunque, il Giudice dell'Unione sta operando il bilanciamento tra i diritti e gli interessi in esame, limitando la tendenza all'utilizzo di strumenti investigativi di tipo massivo che, in nome del contrasto a minacce 'tanto immanenti quanto pulviscolari', finirebbero per imporre regolarmente l'abbassamento del livello di tutela degli interessati i cui dati personali sono oggetto di trattamento.

7. Brevi considerazioni conclusive.

Nella parte iniziale del presente lavoro è stato posto un interrogativo teso a integrarne l'obiettivo finale: se individuato il punto di equilibrio tra impianti normativi sovente confliggenti e circoscritte le politiche securitarie entro il perimetro della proporzionalità, si possa sostenere che protezione dati e *cybersecurity* siano da considerare in rapporto di complementarietà.
A fronte di un contesto giuridico talvolta ancora 'impreparato' ad affrontare i grandi cambiamenti imposti dalla diffusione delle tecnologie digitali e alla luce delle perplessità che inevitabilmente albergano in tutti coloro i quali comprendono che un mercato vasto e redditizio come quello dei dati, è fonte di potere potenzialmente smisurato e incontrollabile in capo a chi detiene quei dati (siano essi soggetti pubblici o privati), non v'è che da sperare che l'impianto normativo volto a garantire una tutela 'forte' del diritto alla protezione dei dati non venga via via svuotato di contenuto.
Se le attività tese a garantire la sicurezza delle reti all'interno dell'U.E. non richiederanno, per il loro espletamento, la sistematica deroga alle regole dettate in tema di protezione dei dati personali, discipline apparentemente confliggenti potrebbero effettivamente rivelarsi complementari l'una rispetto all'altra. Arginando, le politiche securitarie entro limiti prestabiliti, la *cybersecurity*, quale insieme delle attività volte a garantire la sicurezza dello spazio cibernetico, e la protezione dei dati trattati in rete finirebbero così per costituire due facce della stessa medaglia.

ISSN 2036-7821