RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2024 • DOI 10.32091/RIID0158 • articolo sottoposto a peer review • pubblicato in anteprima il 4 lug. 2024
licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo (CC BY NC SA) 4.0 Internazionale

Benedetto Ponti

Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi

Il saggio riflette sulle diverse declinazioni in cui può svolgersi (ed effettivamente si svolge) il rapporto tra cybersecurity e tutela dei dati personali. In particolare, sono individuate tre specifiche declinazioni di questo rapporto, qualificabili rispettivamente in termini di sinergia; di (reciproco) bilanciamento; infine, un rapporto qualificabile in termini di parallelismo. Le diverse sfaccettature del rapporto cybersecurity/tutela dei dati personali non si esauriscono entro questo schema interpretativo. Piuttosto, le tre declinazioni proposte sono individuate quali chiavi di lettura particolarmente interessanti, perché aiutano a cogliere la ricchezza e la densità di tale rapporto. Già in premessa, le chiavi di lettura così proposte tratteggiano i termini di un rapporto niente affatto univoco, e designano una relazione non scontata, né lineare, tra le due grandezze messe a tema. Il saggio si propone anche di dare corpo a questa premessa, corroborando la tesi di un rapporto molto meno diretto e scontato di quanto non si possa ritenere *prima facie*, ciò che implica un livello maggiore di consapevolezza non solo tra gli studiosi e gli addetti ai lavori, ma da parte di tutti gli utenti dei servizi che l'ordinamento appresta a tutela dei dati personali, per un verso, e a tutela della sicurezza cibernetica, per l'altro.

Tutela dei dati personali – Cybersecurity – Sinergia – Bilanciamento – Parallelismo

Synergies, balances, and parallelism between the cybersecurity and personal data protection

In the essay, some declinations of the link between cybersecurity and data protection that may exist – and do exist – are discussed. In particular, three distinct declinations of this relationship are identified, which can be further classified as follows: synergy; (reciprocal) balancing; and finally, a relationship that can be qualified in terms of parallelism. This interpretive scheme does not cover all the aspects of the link between cybersecurity and personal data protection. Rather, the depth and density of this relationship are captured by the three proposed declinations, which are recognized as particularly interesting keys. The terms of a relationship that is by no means unambiguous are outlined in the introduction's keys of interpretation, which also designate a relationship that is neither clear nor linear between the two magnitudes assigned to the topic. The essay aims to provide weight to this assumption by supporting the thesis of a much less clear-cut and direct relationship than one might initially think; this suggests that researchers, practitioners, and all users of the system's services for the protection of cybersecurity and personal data should be aware of this relationship.

Personal data protection – Cybersecurity – Synergy – Balancing – Parallelism

L'Autore è professore associato di Diritto amministrativo presso l'Università degli studi di Perugia

Questo contributo fa parte della sezione monografica *Lo Stato insicuro. Sicurezza e sorveglianza nella cybersocietà,* a cura di Marina Pietrangelo

Sommario: 1. Premessa. – 2. La sinergia tra cybersecurity e tutela dei dati personali. – 3. Il bilanciamento tra cybersecurity e tutela dei dati personali. – 4. Parallelismi tra cybersecurity e tutela dei dati personali.

1. Premessa

Il presente contributo intende evidenziare le diverse declinazioni in cui può svolgersi (ed effettivamente si svolge) il rapporto tra cybersecurity e tutela dei dati personali, da intendersi, entrambe le grandezze, sia in termini di esigenza, di interesse che chiede di essere tutelato, sia con riferimento alla disciplina positiva che è concretamente apprestata a tale fine.

In particolare, vorrei concentrare la mia attenzione su tre specifiche declinazioni di questo rapporto, che potremmo in prima battuta individuare e caratterizzare in questo modo:

– un rapporto qualificabile in termini di sinergia;
– un rapporto qualificabile in termini di (reciproco) bilanciamento;
– un rapporto qualificabile in termini di parallelismo.

Le riflessioni che seguono non hanno la pretesa di esaurire o ricondurre entro questo schema interpretativo tutte le diverse sfaccettature del rapporto cybersecurity/tutela dei dati personali. Piuttosto, chi scrive ritiene che si tratti di chiavi di lettura particolarmente interessanti, perché aiutano a cogliere la ricchezza e la complessità della tematica.

Come si vede, già ad un primissimo sguardo ai "titoli" delle chiavi di lettura proposte, si tratta di declinazioni niente affatto univoche o armoniche tra loro, e che parrebbero designare una relazione non scontata, né lineare, tra le due grandezze. Ciò che mi propongo di fare è anche di dare corpo a questa primissima "impressione", corroborando la tesi di un rapporto molto meno diretto e scontato di quanto non si possa ritenere *prima facie*, ciò che implica un livello maggiore di consapevolezza non solo tra gli studiosi e gli addetti ai lavori, ma da parte di tutti gli utenti di questi "servizi" (in definitiva, tutti i cittadini).

2. La sinergia tra cybersecurity e tutela dei dati personali

La prima declinazione del rapporto tra cybersecurity e tutela dei dati personali che metto a tema è la sinergia. Con questo termine, sintetico, mi riferisco alla circostanza per cui, in primo luogo, l'interesse alla sicurezza dell'ambiente, delle risorse, dei servizi che abilitano il ciberspazio ha ambiti, settori di sovrapposizione (e, dunque, di coincidenza) con l'interesse alla tutela dei dati personali. Detto in modo meno rozzo: l'interesse (pubblico) alla sicurezza del ciberspazio muove nella medesima direzione dell'interesse (di ciascun consociato) alla tutela dei dati personali, nella misura in cui la protezione dell'ambiente in cui i dati personali sono destinati ad essere raccolti, conservati, fruiti è funzionale alla tutela del diritto (dei diritti, al plurale) sottesi alla protezione dei dati. Non si tratta, ben inteso, di una coincidenza piena (né sul piano quantitativo, né sul piano qualitativo). E tuttavia, appare evidente che, nella misura in cui la tutela dei dati personali si sostanzia (ad esempio) nel rispetto dei principi sul trattamento di cui all'art. 5 del GDPR, un ambiente sicuro costituisce un fattore che abilita e rafforza il rispetto di questi principi.

Si pensi al principio di *limitazione della finalità del trattamento*: la possibilità di conservare, gestire e trasmettere dati personali in modo sicuro (o, quantomeno, adeguatamente presidiato rispetto a intrusioni) costituisce di per sé un fattore che rende meno probabile l'appropriazione e l'uso dei dati personali per fini diversi da quelli ammessi dalla vigenza del principio di limitazione della finalità. Oppure, si pensi al principio di *minimizzazione*

dei dati: la disponibilità di tecnologie e soluzioni di crittografia (sviluppate e gestite a fini di cibersicurezza) consente più agevolmente di trattare i dati in conformità con questo principio.

O, ancora, si pensi al principio di *integrità e riservatezza*, che costituisce forse la traduzione più aderente delle istanze della cybersecurity nell'ambito della disciplina generale di tutela dei dati personali. E si potrebbe continuare.

Il rapporto di sinergia (in quanto tale) vale anche nel senso opposto, ovvero se osserviamo il rapporto dal punto di vista della cybersecurity. Valga quanto detto adesso con riferimento al principio (un *principio sul trattamento dei dati personali*) di *integrità e riservatezza*. La realizzazione di soluzioni organizzative, procedurali e tecnologiche finalizzate a mitigare il rischio di intrusioni malevole e a contenerne effetti e ricadute, contribuisce largamente a dare seguito e sostanza agli obblighi di sicurezza che gravano sul titolare e sul responsabile del trattamento, per effetto di quanto disposto dall'art. 32 del GDPR.

Se questa sinergia può apparire scontata, con riferimento alle istanze di riservatezza, limitazione, protezione dei dati da intrusioni esterne (la privacy come istanza classica di *esclusione*), va sottolineato che essa trova riscontro anche rispetto all'altro obiettivo della disciplina del GDPR, quello della circolazione dei dati personali. Infatti, un ambiente comunicativo sicuro, perché adeguatamente protetto da minacce esterne, costituisce un fattore indispensabile a favorire la circolazione dei dati (che presuppone il transito degli stessi, quando non il loro stoccaggio in infrastrutture di condivisione).

Dunque, esistono solidi argomenti a dimostrazione di una sinergia (tutt'altro che sorprendente) sul piano dei fini (gli interessi tutelati) e delle discipline positive.

Ma questa sinergia si può riscontrare anche su un piano differente, ovvero quello dell'*approccio* e del *modello di regolazione* adottato a livello di Unione europea. Come è stato efficacemente segnalato in dottrina[1], infatti, se si mettono a confronto la disciplina di tutela dei dati (il GDPR) e alcune fondamentali discipline in materia di cybersicurezza, quali la direttiva NIS (e NIS2), la PSD2 (la direttiva sui pagamenti digitali) e la direttiva eIDAS (la direttiva sull'identificazione elettronica e i servizi fiduciari), è possibile riscontrare alcune rilevanti *isomorfie* negli approcci regolatori adottati.

Ad esempio, l'*analisi del rischio* come presupposto per la taratura delle misure di protezione da adottare è comune al GDPR come pure alla disciplina PSD2 e alla direttiva NIS2.

Ancora, il principio secondo il quale le esigenze di tutela dei dati personali andrebbero anticipate e inserite nella stessa progettazione dei sistemi (*privacy by design* e *by default*) si ritrova anche nella disciplina PSD2 e in quella eIDAS[2].

Il principio per cui ogni *data breach* deve essere opportunamente notificato (*reporting obligation*) è recepito in ciascuna delle discipline richiamate qui sopra, come pure le esigenze di assicurare adeguate procedure di *Business continuity* e di *Disaster recovery*.

Si tratta, come si può notare, di sinergie che si collocano su un piano procedurale e operativo, e che certamente possono aiutare a leggere i diversi *testi regolatori* non come corpi separati (che danno luogo ad una normativa frammentaria), ma piuttosto come sistemi coerenti ed integrati[3]. Ciò che appare particolarmente utile sul lato delle imprese (come pure delle amministrazioni) che devono sostenere i costi della *compliance*, e che da una prospettiva di questo genere possono trarre vantaggio (e non solo sul piano delle economie di spesa, ma anche su quello della efficacia delle soluzioni così implementate). Ciò è tanto più importante, se si considera che il principio del *risk assessment* – e più in generale, l'approccio regolatorio fondato sulla adeguatezza delle misure adottate e la connessa accountability del titolare (e del responsabile) del trattamento – è tuttora vissuto da una parte significativa del mondo imprenditoriale (con specifico, sebbene non esclusivo, riferimento al settore della media e piccola impresa, e dell'artigianato) come fattore di incertezza, che rende più complesso

1. Mantelero-Vaciago 2020; Viggiano 2021.
2. Evidenziano l'estensione di tale approccio alla regolamentazione dell'AI, *ex multis*, Andraško-Mesarčík-Hamuľák 2021.
3. Angelini-Ciccotelli-Franchina et al. 2020.

pianificare ed ammortizzare i costi e implementare le soluzioni adeguate[4]. Un approccio integrato e sistematico, che riguardi i diversi aspetti di *compliance* qui indicati, ne renderebbe più efficiente il recepimento e l'applicazione[5]. Ciò che però sembra richiedere una forte collaborazione, a monte e a valle, anche da parte delle (plurime) autorità di settore coinvolte.

3. Il bilanciamento tra cybersecurity e tutela dei dati personali

Il perseguimento della sicurezza nel ciberspazio può porsi, però, anche come istanza/finalità/interesse idoneo a limitare/ridurre il livello di protezione assicurato ai dati personali. In questo (diverso) schema interpretativo, cioè, il perseguimento dell'una finalità (la sicurezza – anche – nel ciberspazio) entra in relazione di *bilanciamento* con l'esigenza di tutela dei dati personali, tale per cui il peso, l'importanza, la gravità degli interessi sottesi può comportare una *diminutio* del livello di tutela assicurato alla protezione dei dati personali[6]. Sia chiaro, anche la disciplina "ordinaria" di tutela dei dati personali (quella disposta con il GDPR) integra un'operazione di bilanciamento, tra tutela dei dati personali e gli altri interessi in virtù dei quali sono fissati (in quella disciplina) i presupposti, i principi e i diritti connessi al trattamento dei dati. In altre parole, non essendo la tutela dei dati personali un diritto assoluto, ogni normativa che ne disciplina il trattamento comporta in ogni caso una qualche forma di bilanciamento.

Pertanto, qui faccio riferimento ai casi in cui la disciplina positiva di tutela dei dati, qualora il trattamento sia giustificato da esigenze di sicurezza (e, quindi, anche di cibersicurezza), si discosta da quella generale, proprio in ragione del fatto che – per tali finalità – si giustificato (sono giudicati legittimi) bilanciamenti differenti (rispetto a quelli recepiti nella disciplina ad applicazione generale residuale, quale è quella del GDPR) tra i due interessi in campo.

Come noto, una fondamentale ragione a giustificazione di questo diverso bilanciamento dipende dalla riserva esclusiva in capo agli Stati membri della materia *sicurezza nazionale*, così come sancita nell'art. 4 del TUE[7], e più in generale dal rispetto delle funzioni essenziali dello Stato, tra le quali certamente le funzioni connesse alla prevenzione, all'indagine e al perseguimento di reati.

Ciò comporta (o contribuisce a determinare) due ordini di conseguenze. In primo luogo, con riferimento alla disciplina del trattamento dei dati personali, quando questa concerne le materie attinenti alla prevenzione, all'indagine e al perseguimento di reati, il rispetto delle funzioni essenziali dello Stato comporta il ricorso ad uno strumento di armonizzazione quale la direttiva, così da lasciare margini significativi allo Stato membro per adattare i principi in materia di tutela dei dati personali alle specificità nazionali. In secondo luogo, con riferimento alla disciplina della cybersecurity, quando questa implica il compimento di funzioni che attengono alla tutela della sicurezza nazionale, ciò la fa ricadere al di fuori dell'ambito coperto dalla relativa disciplina dell'Ue. In questo senso, è significativo quanto ribadito da ultimo dalla direttiva NIS2, all'art. 2, che ne regola l'ambito di applicazione[8].

Entro queste coordinate, si aprono dunque spazi per un bilanciamento tra i valori in gioco in cui la

4. Kaiser 2023; Härting-Kaim-Klamm-Kroneberg 2021.
5. Nwankwo-Stauch-Radoglou-Grammatikis et al. 2022.
6. van de Poel 2020; Christen-Gordijn-Weber et al. 2017.
7. «[L'Unione europea] rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro».
8. Nello specifico, va preso in considerazione il testo dei parr. 6 e 7 dell'art. 2, dove si statuisce che [6] «La presente direttiva lascia impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e il loro potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico», e che [7] «La presente direttiva non si applica agli enti della pubblica amministrazione che svolgono le loro attività nei settori della sicurezza nazionale, della pubblica sicurezza o della difesa, del contrasto, comprese la prevenzione, le indagini, l'accertamento e il perseguimento dei reati».

tutela dei dati personali può subire limitazioni entro margini più ampi di quelli contemplati dal GDPR.

Ad esempio quando si tratti di contrastare i *cyber crime*, lo spazio di manovra riconosciuto al legislatore nazionale nel limitare i diritti dell'interessato è più ampio: sia in ragione dello strumento normativo utilizzato (la direttiva), sia in ragione delle specifiche esigenze connesse allo svolgimento delle indagini (oltre che a quelle connesse alla fase più propriamente processuale-penale). Si consideri poi che il novero dei diritti riconosciuti all'interessato è meno esteso di quello sancito nel GDPR, e che sono contemplate ampie ipotesi che ne giustificano la limitazione.

Significativi esempi, quanto alla esplorazione di questi margini di manovra, si trovano nella recente l. n. 137/2023 di conversione del d.l. 105/2023. In particolare, l'art. 2-*bis* ha introdotto un comma aggiuntivo all'art. 17 del d.l. 14 giugno 2021, n. 82 (istitutivo dell'Agenzia per la cybersicurezza nazionale), in ragione del quale l'Agenzia è tenuta a trasmettere al procuratore nazionale antimafia e antiterrorismo i dati, le notizie e le informazioni rilevanti per l'esercizio delle funzioni di coordinamento delle indagini, di cui all'art. 371-*bis* del codice di procedura penale.

Di più acuto rilievo (quanto a distanziamento dai criteri ordinari di bilanciamento) è la questione relativa a quella che in dottrina è variamente indicata come *data retention saga*[9]. Come noto, a partire dalla vicenda culminata nella notissima sentenza *Digital Rights Ireland* della Corte di giustizia dell'Ue[10], si è sviluppato nel corso degli anni una sorta di "braccio di ferro" tra gli Stati membri – desiderosi di poter sfruttare in modo pieno le potenzialità di indagine abilitate dalla conservazione integrale dei (meta) dati di traffico delle comunicazioni elettroniche, compresa l'ubicazione (con riferimento alla telefonia mobile) – e la resistenza opposta in particolare dalla giurisprudenza delle corti superiori (CGUE e Corte EDU), tesa piuttosto a ricondurre l'ambito di praticabilità di una simile ingerenza/limitazione del diritto alla tutela dei dati personali entro i parametri coerenti con un giudizio di stretta proporzionalità.

Dal nostro punto di vista (nell'ottica, cioè, del bilanciamento tra esigenze di cybersecurity e di tutela dei dati personali), questa *querelle* è significativa (ed indicativa) sotto molteplici punti di vista.

In primo luogo, occorre tenere conto della circostanza per cui anche in questo caso viene in rilievo un atto normativo (la direttiva *ePrivacy*) che – per sua natura – apre spazi di attuazione differenziata nei diversi Stati membri, e che pertanto accetta come leciti bilanciamenti anche parzialmente differenziati tra loro. Tanto più che l'"esordio" di tale *querelle* si è svolto con riferimento ad un atto normativo dell'Unione (la direttiva 2006/24/CE, volta proprio ad armonizzare le legislazioni nazionali in materia di *data retention*), cosicché in tale occasione la Corte di giustizia ha fatto diretta applicazione dei principi di cui agli artt. 7, 8 e 52 della Carta dei diritti fondamentali dell'Ue. Sebbene ciò abbia comportato la definizione di un test di proporzionalità sufficientemente stringente (la disciplina di cui trattasi «deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura *de qua* e impongano requisiti minimi in modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati»; e quindi: una perimetrazione dei dati da conservare commisurata alla gravità dei reati che si intendono contrastare; la fissazione di criteri oggettivi che permettano di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore a fini di prevenzione, di accertamento o di indagini penali; tempi di conservazione proporzionati in relazione alla tipologia di dati e alla loro utilità potenziale in funzione dell'obiettivo perseguito).

Resta però il fatto che la traduzione di un test di tale sorta nei termini di una disciplina positiva lascia spazio a fattispecie applicative anche molto differenziate tra loro (ciò che le vicende successive si sono incaricate di confermare).

Si noti, per altro, che sebbene la *finalità* ultima di tali discipline sia – appunto – *l'indagine*, *l'accertamento* e *il perseguimento di reati gravi*, l'oggetto delle normative si colloca in momento antecedente, e consiste appunto negli *obblighi di conservazione* posti in capo *agli operatori delle comunicazioni elettroniche*, funzionali ad abilitare la disponibilità

9. Bergholm 2021; Grzelak 2016.

10. Cause C-293/12 e C-594/12 riunite.

di tali dati per le eventuali finalità di indagine/accertamento/perseguimento dei reati. Si tratta, cioè, di un trattamento posto in essere in prima battuta dagli operatori di mercato, su dati generati nella ordinaria prestazione del servizio. A costoro possono, dunque, essere imposti trattamenti *differenziati*, che comportano un diverso (meno intenso) livello di applicazione quantomeno dei principi di "minimizzazione" e di "limitazione della conservazione".

Nella misura in cui tali limitazioni sono giustificate anche in vista del perseguimento dei c.d. *cybercrime* (e, quindi, anche in funzione di sicurezza cibernetica), ciò dimostra l'operatività di un bilanciamento *differenziato*.

In secondo luogo, nel corso del "braccio di ferro" sulla *data retention*, la giurisprudenza, tanto della Corte di Lussemburgo quanto della Corte di Strasburgo, ha finito per legittimare ipotesi di *bulk data retention*, qualora vengano in considerazione «esigenze di salvaguardia della sicurezza nazionale», ovvero proprio quell'ambito materiale che l'art. 4, par. 2 del TUE riserva alla esclusiva competenza degli Stati membri. Ora, se è vero che a questo riguardo la Corte di giustizia ha chiarito – in premessa – che «una misura nazionale […] adottata a fini di salvaguardia della sicurezza nazionale non può comportare l'inapplicabilità del diritto dell'Unione e dispensare gli Stati membri dal necessario rispetto di tale diritto», ciò nondimeno «l'interesse primario di tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società, [interesse che] comprende la prevenzione e la repressione di attività tali da destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese, e in particolare da minacciare direttamente la società, la popolazione o lo Stato in quanto tale, quali in particolare le attività di terrorismo» – ovvero l'interesse alla sicurezza nazionale – «[è] idoneo a giustificare misure che comportino ingerenze nei diritti fondamentali più gravi di quelle che potrebbero giustificare altri obiettivi»[11]. In questi casi, cioè, la Corte ammette l'individuazione di un punto di equilibrio in cui il sacrificio dei diritti a tutela dei dati personali può (legittimamente) risultare più marcato. Tale impianto argomentativo, che distingue la praticabilità di misure di sorveglianza generalizzata in caso di minacce concrete alla sicurezza nazionale (sebbene al netto di alcune garanzie procedurali[12], quali il controllo da parte di una autorità indipendente) e la loro (sostanziale) interdizione nel caso dell'ordinario perseguimento di reati pure "gravi", è stato ribadito da ultimo, nella sentenza *Commissioner of An Garda Síochána*, del 2022[13].

Analogo è l'approccio che emerge dalla più recente giurisprudenza della Corte EDU. Nel caso *Big Brother Watch and Others v. the United Kingdom*, deciso dalla Grand Chambre nel maggio del 2021, la Corte era chiamata a valutare la compatibilità con l'art. 8 della Carta CEDU (letto alla luce della Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale) della legislazione inglese allora vigente (il *Regulation of Investigatory Powers Act 2000*, in seguito abrogato e sostituito dall'*Investigatory Powers Act* del 2016). Tale disciplina contemplava misure quali: l'intercettazione massiccia delle comunicazioni (c.d. *bulk interception*) su mandato del governo; lo scambio di dati tra agenzie di intelligence straniere; l'acquisizione dei dati di comunicazione da parte di service providers (*data retention*). La Corte di Strasburgo non esita a riconoscere che tali misure di sorveglianza rivestono «un'importante capacità tecnologica di identificare nuove minacce nel dominio digitale» e che «l'intercettazione massiva è di vitale importanza per gli Stati contraenti nell'individuare le minacce alla loro sicurezza nazionale»[14]. Anche sulla scorta di queste considerazioni, la Corte nota come l'art. 8 della Convenzione «non proibisce l'uso di intercettazioni di massa per proteggere la sicurezza nazionale e altri interessi nazionali essenziali contro gravi minacce esterne» e che «gli Stati dispongono di un ampio margine di apprezzamento nel decidere quale tipo di regime di intercettazione sia necessario», margine temperato da alcune garanzie procedurali di

11. Cfr. CGUE, C-511/18 e C-512/18 *La Quadrature du Net*, nonché C-623/17 *Privacy International*.
12. Zalnieriute 2021.
13. Cfr. CGUE, C-140/20.
14. Cfr. ECHR, *Big Brother Watch and Others vs. The United Kingdom* (Applications n. 58170/13, 62322/14 and 24960/15).

base (garanzie la cui assenza ha determinato il giudizio di violazione dell'art. 8, nel caso concreto)[15].

Come si vede, anche in questo caso le finalità connesse alla protezione della sicurezza nazionale, giustificano un punto di equilibrio (che gli Stati possono individuare, in esito all'esercizio del *wide margin of appreciation* loro accordato) nel quale viene giustificato un (ben) più intenso grado di ingerenza sulla protezione dei dati personali rispetto allo standard fissato con il GDPR (o anche nella stessa direttiva 680/2016), in termini convergenti con quanto emerso nella giurisprudenza della CGUE («the two Courts are converging rather than diverging in their recent jurisprudence concerning the data retention saga»[16]).

Nella misura in cui la sicurezza nazionale (oggetto di protezione) si configura anche (soprattutto, nei tempi odierni?) come cybersicurezza, emergono molto bene i profili di bilanciamento: il perseguimento della (cyber)sicurezza nazionale è suscettibile di giustificare più forti/rilevanti limitazioni dei diritti degli interessati e degli stessi principi che reggono (ordinariamente) il regime di tutela dei dati personali.

Ma c'è forse qualcosa di più da notare. Le misure mediante le quali si articola la tutela della sicurezza nazionale (anche quelle oggetto di attenzione della giurisprudenza appena richiamata) si configurano, tendenzialmente, come trattamenti automatizzati, che sfruttano le potenzialità tecnologiche, conoscitive, investigative, di intelligence, e che presuppongono un uso dei dati personali *in contraddizione* con i principi sul trattamento lecito (ai sensi, ad esempio, del GDPR o della direttiva 680/2016), quali il principio di limitazione della finalità del trattamento, il principio di minimizzazione dei dati, o quello di limitazione della conservazione. Questa è la ragione per la quale la loro *ammissibilità* richiede un diverso punto di equilibrio (rispetto a quello codificato nel GDPR e anche nella direttiva 680/2016). Nello stesso tempo, si tratta molto spesso di sviluppare e applicare misure di cybersecurity capaci di muoversi sullo stesso piano di quelle con le quali sono perpetrati gli attacchi alla sicurezza nazionale (alla stregua del proverbio "*a brigante, brigante e mezzo*", ovvero "*combattere con le armi del nemico*"). E, si noti, non si tratta solo dell'ambito connesso alla materia della difesa (verso nemici "esterni"), declinabile nei termini del *cyberwarfare*, ma anche della *sicurezza interna*[17].

In altre parole, qui ci troviamo di fronte ad un bilanciamento (a sfavore della tutela dei dati personali) applicato perché le esigenze di cybersicurezza siano soddisfatte mediante la predisposizione di mezzi adeguati, perché uguali e contrari a quelli che la mettono in pericolo. Si affacciano, così, (sotto vesti non del tutto inedite) questioni connesse alla tematica classica della *democrazia protetta*: ovvero se e quanto sia possibile non solo *comprimere*, ma addirittura *contraddire* la tutela di diritti fondamentali (quale in questo caso il diritto alla tutela dei dati personali) per fare fronte a minacce esistenziali alla convivenza organizzata[18].

4. Parallelismi tra cybersecurity e tutela dei dati personali

Il terzo rapporto che vorrei evidenziare è declinato in termini di parallelismo, e per illustrarlo vorrei concentrarmi sull'attore pubblico, in particolare le amministrazioni pubbliche. Nella progettazione, realizzazione e implementazione di soluzioni (più o meno) automatizzate che implicano il trattamento di dati personali, così come nel caso di procedure, soluzioni e misure per la cybersecurity, le amministrazioni si trovano nella condizione (necessitata, per una serie plurima di ragioni più o

15. Naddeo 2022; «the real significance of the case lies in endorsing the legality of mass surveillance. Despite the finding of violation, the majority of the GC declared, just as the regular Chamber did in 2018, that mass-surveillance is not, in principle, unlawful and/or disproportionate».

16. Tzanou-Karyda 2022.

17. Cfr., da ultimo, CGUE, *Valstybės sienos apsaugos tarnyba*, causa C-72/22 PPU, nella quale la Corte osserva che la nozione di sicurezza nazionale «comprende la sicurezza interna di uno Stato membro e la sua sicurezza esterna e, pertanto, il pregiudizio al funzionamento delle istituzioni e dei servizi pubblici essenziali nonché la sopravvivenza della popolazione, come il rischio di perturbazioni gravi dei rapporti internazionali o della coesistenza pacifica dei popoli, o ancora il pregiudizio agli interessi militari, possono ledere la pubblica sicurezza».

18. Broeders-Cristiano-Weggemans 2023.

meno storicamente determinate) di interagire con il mercato e i suoi attori.

Nel caso del trattamento dei dati personali, perché questo costituisce un risvolto necessitato di qualsiasi soluzione volta a supportare o direttamente concretizzare l'esercizio di funzioni pubbliche mediante il ricorso alle c.d. tecnologie digitali (per usare un termine *riassuntivo*). Questo rapporto è caratterizzato da rilevanti asimmetrie conoscitive (oltre che operative), anche con specifico riferimento agli impatti delle soluzioni progettate/adottate in termini di compatibilità con la disciplina sul trattamento dei dati personali[19].

Non dissimile è il tipo di rapporto che si instaura con i soggetti che forniscono consulenza, soluzioni e prodotti da destinare alla tutela della sicurezza cibernetica delle amministrazioni. Anche qui, il ricorso al mercato è sostanzialmente necessitato, ed è parimenti caratterizzato da rilevanti asimmetrie[20]. Già questo aspetto indica un evidente parallelismo (per altro in qualche modo implicito nel rapporto di sinergia di cui si è già detto).

Tuttavia, le analogie non si fermano a questa constatazione (di natura prevalentemente *fattuale*). Se si guarda a come tale rapporto (asimmetrico) può essere governato dalla parte "debole", si scorgono ulteriori similitudini. Un'alternativa possibile è quella di strutturare il rapporto in termini gerarchici, basati sullo schema del *command and control*, nel tentativo di colmare, mediante l'esercizio dell'autorità, una capacità di controllo che l'asimmetria informativa impedirebbe di esercitare. Si tratta di una soluzione che presenta notevoli controindicazioni: tende ad irrigidire le soluzioni così predisposte (condannandole spesso a una scarsa effettività, e comunque a una rapida obsolescenza), impedisce di sfruttare appieno lo stato dell'arte in termini di ricerca e sviluppo e costituisce un incentivo per il partner privato a puntare su commesse quantitativamente importati (sotto il profilo del prezzo) piuttosto che qualitativamente qualificate. Soprattutto, tende a preservare e consolidare l'asimmetria informativa, rafforzando la condizione di junior partner (sostanziale) in cui l'amministrazione si trova ad operare.

Un approccio alternativo è quello che invece punti a strutturare il rapporto in modo più paritario, su base collaborativa e aperta[21]. Un approccio che può consentire di evitare molte delle controindicazioni prima evidenziate, e avere così soluzioni più flessibili, capaci di incorporare in modo tempestivo le innovazioni, e quindi qualitativamente qualificate). Tuttavia per poter essere perseguito, tale approccio richiede alcune pre-condizioni. In primo luogo, occorre che l'amministrazione disponga di effettivi margini entro i quali sviluppare la collaborazione, ciò che implica una serie di scelte in capo al legislatore, in termini di definizione del framework operativo. Il nuovo Codice dei contratti pare muoversi in questa direzione, come pure coerenti con questa esigenza appaiono le modifiche al Codice privacy in materia di presupposti di liceità per il trattamento dei dati personali per l'esercizio di funzioni pubbliche[22]. Diversamente, la dottrina maggioritaria segnala come l'architettura nazionale in materia di cybersecurity rifletta un'impostazione metodologica ancora troppo legata al modello dell'*intelligence*, e quindi poco o per nulla caratterizzata in termini di collaborazione e di apertura[23].

Un ulteriore presupposto, indispensabile perché la collaborazione (qualora possibile) non si trasformi in una *colonizzazione* da parte degli attori di mercato[24], consiste nel dotare le amministrazioni (il sistema amministrativo) di competenze e capacità utili per potersi confrontare in modo consapevole ed attrezzato con i partner privati. Sotto questo profilo, va evidenziato il ruolo che possono svolgere le università e le altre istituzioni della ricerca pubblica, e vale la pena sottolineare (in questo senso) la *buona pratica* rappresentata dal consorzio Cini[25], come esperimento (di successo) non solo nel creare una

19. Bharosa 2022; Taylor 2021.

20. Previti 2022.

21. Barone 2006.

22. Ponti 2023.

23. Serini 2023; Rossa 2023; Previti 2022; Barone 2006.

24. Mazzuccato-Collington 2023; Taylor 2021.

25. Cfr. il sito del consorzio.

rete, ma anche nel promuovere azioni finalizzate alla maturazione e al trasferimento di conoscenze e competenze cui le amministrazioni possono (eventualmente) attingere, per strutturarsi come player *attivi* e *attrezzati* del sistema di sicurezza cibernetica nazionale. Ciò che richiede, evidentemente, investimenti importanti, soprattutto sul fronte del capitale umano. È, questo, un capitolo distinto, e altrettanto importante, che non è possibile nemmeno sfiorare in questa sede.

Riferimenti bibliografici

J. Andraško, M. Mesarčík, O. Hamuľák (2021), *The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework*, in "AI & Society", vol. 36, 2021, n. 2

M. Angelini, C. Ciccotelli, L. Franchina et al. (2020), *Italian National Framework for Cybersecurity and Data Protection*, in L. Antunes, M. Naldi, G. Italiano, K. Rannenberg, P. Drogkaris (eds.), "Privacy Technologies and Policy. APF 2020. Lecture Notes in Computer Science", Springer, vol. 12121

A. Barone (2006), *Il diritto del rischio*, Giuffrè, 2006

N. Bharosa (2022), *The rise of GovTech: Trojan horse or blessing in disguise? A research agenda*, Government Information Quarterly, vol. 39, 2022, n. 3

J. Bergholm (2021), *The Data Retention Saga Continued–from Tele2 Sverige to Privacy International and La Quadrature du Net*, in "JFT", vol. 2021, n. 2

D. Broeders, F. Cristiano, D. Weggemans (2023), *Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy*, in "Studies in Conflict & Terrorism", vol. 46, 2023, n. 12

M. Christen, B. Gordijn, K. Weber et al. (2017), *A Review of Value-Conflicts in Cybersecurity: An assessment based on quantitative and qualitative literature analysis*, in "Orbit, An Online Journal for Responsible Research and Innovation in ICT", vol. 1, 2017, n. 1, pp. 1-19

A. Grzelak (2016), *Data Retention Saga Continues: Decision of the Polish Constitutional Tribunal of 30 July 2014 in Case K 23/11*, in "European Public Law", vol. 22, 2016, n. 3

R.C. Härting, R. Kaim, N. Klamm, J. Kroneberg (2021), *Impacts of the New General Data Protection Regulation for small-and medium-sized enterprises*, in X.S. Yang, R.S. Sherratt, N. Dey, A. Joshi (eds.), "Proceedings of Fifth International Congress on Information and Communication Technology: ICICT 2020", Springer, vol. 1, 2021, pp. 238-246

M. Mazzuccato, R. Collington (2023), *The Big Con: How the Consulting Industry Weakens our Businesses, Infantilizes our Governments and Warps our Economies*, Penguin, 2023

E. Kaiser (2023), *The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations*, in "Media laws", 2023, n. 1

A. Mantelero, G. Vaciago (2022), *Reconciling Data Protection and Cybersecurity: An Operational Approach for Business Sector*, in R. Senigaglia, C. Irti, A. Bernes (eds.), "Privacy and Data Protection in Software Services", Springer, 2022

G. Naddeo (2022), *Il difficile bilanciamento tra sicurezza nazionale e tutela dei diritti fondamentali nella "data retention saga" dinanzi alla Corte di giustizia*, in "Freedom, Security & Justice: European Legal Studies", 2022, n. 2, pp. 188-217

I. Nwankwo, M. Stauch, P. Radoglou-Grammatikis et al. (2022), *Data Protection and Cybersecurity Certification Activities and Schemes in the Energy Sector*, in "Electronics", vol. 11, 2022, n. 6, p. 965

B. Ponti (2023), *Attività amministrativa e trattamento dei dati personali. Gli standard di legalità tra tutela e funzionalità*, FrancoAngeli, 2023

L. Previti (2022), *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in "federalismi.it", 2022, n. 25

S. Rossa (2023), *Cybersicurezza e pubblica amministrazione*, Editoriale Scientifica, 2023

F. Serini (2023), *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in "Rivista italiana di informatica e diritto", 2023, n. 2

L. Taylor (2021), *Public Actors Without Public Values: Legitimacy, Domination and the Regulation of the Technology Sector*, in "Philosophy and Technology", vol. 34, 2021

M. Tzanou, S. Karyda (2022), *Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga?*, in "European Public Law", vol. 28, 2022, n. 1

I. van de Poel (2020), *Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security*, in M. Christen, B. Gordijn, M. Loi (eds.), "The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology", Springer, vol 21, 2020

M. Viggiano (2021), *Cybersecurity and Data Protection in European Union Policies and Rules: The NIS Directive and the GDPR Synergy*, in G. De Minico, O. Pollicino (eds.), "Virtual Freedoms, Terrorism and the Law", Routledge, 2021

M. Zalnieriute (2021), *Procedural Fetishism and Mass Surveillance under the ECHR. Big Brother Watch v. UK*, in "VerfassungsBlog", 2 June 2021