CYBERSICUREZZA E PROTEZIONE DEI DATI PERSONALI[1]

Pasquale Stanzione

1. **Il contesto**

1. Partirei da un dato essenziale. In un contesto "multidominio", la cybersecurity è una delle componenti essenziali della sicurezza, dall'importanza progressivamente crescente. Al contempo, la protezione dei dati è un presupposto determinante e sinergico della sicurezza, in particolare cibernetica. L'intero Regolamento generale sulla protezione dei dati si fonda sulla valutazione del rischio connesso alla gestione dei dati personali, delle vulnerabilità e dei deficit infrastrutturali dei sistemi che li ospitano e impone misure, di sicurezza, appunto, volte a prevenire violazioni e a contenerne il pregiudizio eventualmente derivatone.

   A ciò provvede, in particolare, l'istituto della notifica delle violazioni di dati personali che consente al Garante di prescrivere le misure idonee a limitare il danno suscettibile di derivare, ai vari soggetti interessati, dal *data breach*. E' frequente che le violazioni di dati personali integrino anche incidenti di sicurezza rilevanti, appunto, in termini di cybersecurity e viceversa.

   Questo dimostra, ancora una volta, quanto sia rilevante la sinergia tra protezione dei dati e cybersicurezza, pur nell'ambito di una chiara distinzione tra le materie: una centrata sulla tutela di un diritto fondamentale della persona, l'altra di un interesse generale dello Stato.

Ci sono studi, approfondimenti, discipline che restituiscono davvero il senso del presente e lanciano uno sguardo, mai miope, sul futuro. E lo fanno, più e meglio di altri, perché colgono il senso profondo del reale, le sue dinamiche, persino le sue contraddizioni. La protezione dei dati è certamente una di queste discipline, capace come poche altre di descrivere il rapporto tra diritto e tecnica, nella continua rincorsa del primo a normare i mutamenti che la seconda induce nella vita individuale e collettiva.

E'questo, infatti, il terreno elettivo per saggiare la tenuta del diritto rispetto alla tecnica e riportare l'uomo al centro di uno sviluppo tecnologico che rischia, altrimenti, di prescindere da ogni orizzonte di senso.

Il grado di dinamismo e di continua evoluzione di questa materia è tale che, in meno di sei mesi e pur dopo la "pietra miliare" della sentenza Schrems II del luglio 2020, la Corte di giustizia europea ha emesso addirittura tre sentenze su temi cruciali, quale l'effettiva univocità del consenso on line, il rapporto tra privacy e sicurezza nazionale, la *data retention* in rapporto al ruolo del pubblico ministero.

Questo dimostra come in una materia, quale quella in analisi, esposta ad una incessante evoluzione interpretativa, applicativa, al continuo confronto della norma con fattispecie concrete sempre nuove e dalle caratteristiche inedite, l'interprete abbia un bisogno essenziale di guide, di strumenti capaci di orientarne l'analisi e la scelta tra le molte opzioni spesso possibili, tra i vari significati che la stessa disposizione può sostenere. Di qui la funzione insostituibile di questa tipologia di corsi e di approfondimenti; tanto più preziosa rispetto a una materia che ha conosciuto, accanto alle molte e importanti innovazioni del formante giurisprudenziale, la "rivoluzione" del Regolamento generale sulla protezione dei dati e delle relative norme nazionali di adeguamento, di carattere "interstiziale", nonché le rilevantissime novità della, meno nota ma non meno importante, direttiva 2016/680, sulla protezione dei dati nei settori della giustizia penale e della polizia.

In una cornice normativa così complessa, è dunque quantomai essenziale adottare - proprio come questo corso, anche solo dalla scelta dei temi, suggerisce - una prospettiva sinottica, che riconduca

[1] Testo della *Lectio magistralis* tenuta presso la Camera di Commercio di Salerno il 5 maggio 2025.

costantemente la singola disposizione all'interno del contesto più ampio in cui si colloca, evitando di considerare una sola *aliqua particula,* come già diceva Celso, avulsa dal sistema. E questo soprattutto per cogliere, di tale straordinario diritto - mai "tiranno" - l'essenziale funzione sociale nel bilanciamento con gli altri interessi giuridici rilevanti, ricordando che la tecnica - come afferma il Gdpr rispetto al trattamento dei dati - deve porsi "al servizio dell'uomo".

La disciplina di protezione dei dati nasce infatti e si sviluppa intorno all'esigenza di coniugare dignità della persona e libertà d'iniziativa economica; garanzie individuali e innovazione tecnologica; libertà della persona ed esigenze di giustizia, di sicurezza, di trasparenza, d'informazione.

L'accesso alla rete è divenuto presupposto necessario di effettività dei diritti fondamentali e dunque esso stesso diritto fondamentale. La sua costituzionalizzazione è presente nel dibattito dottrinale e giurisprudenziale. Si tratta di superare il *digital divide* che rappresenta, oggi, una delle diseguaglianze più inaccettabili e che riproduce e amplifica le vulnerabilità più tradizionali.

E se il divario digitale costituisce uno dei limiti più rilevanti, sotto il profilo egalitario e inclusivo del processo di digitalizzazione della vita privata e pubblica, esso tuttavia è caratterizzato nell'ora presente da alcune distorsioni che alterano profondamente la natura della rete, rischiando di tradirne la promessa originaria di democraticità e di pluralismo, in primo luogo informativo.

Il combinato disposto del *microtargeting* informativo - come metodo di selezione delle notizie da proporre all'utente - e della diffusione in rete di contenuti falsi oltre che illeciti, spacciati per verità alternative, rischia infatti di rendere quella che è nata come la più grande e aperta *agorà* della storia una somma di *enclave*s, zone ad accesso limitato (Zygmunt Bauman).

Per eterogenesi dei fini, una società, quella digitale, che ha visto cadere i confini di Stati e di sistemi ordinamentali grazie alla connessione globale e all'accesso a ogni sorgente informativa ovunque presente, rischia però di indurre una sorta di riflesso autistico nelle relazioni intersoggettive, tale da evitare il confronto con l'altro-da-sé, di annullare il *Mit-dasein* di Martin Heidegger.

Questa sorta di autismo informativo, che frantuma l'informazione in miriadi di "cascate informative" autoreferenziali e personalizzate su base algoritmica, determina essenzialmente due implicazioni di rilievo.

La prima, sul piano socio-politico, attiene alla polarizzazione estremistica, fin quasi una balcanizzazione, delle posizioni espresse e formate in rete, con il rifiuto della complessità del pensiero, in favore di uno spontaneismo troppo spesso aggressivo e ostile alle differenze. Di qui anche populismi, *hate speech* e una generale mutazione della politica da centripeta in centrifuga, con la tendenza diffusa alla costruzione di identità in chiave oppositiva e polemica.

La seconda implicazione concerne il modo in cui si forma l'opinione pubblica, in particolare politica. Per effetto della "bolla di filtri" e del *microtargeting,* la stessa ricerca di informazioni, di notizie e di tutto ciò che forma l'opinione politica di ciascuno, rischia di essere tutt'altro che neutra rispetto alle proprie precomprensioni, *Vorverstellungen* alla Joseph Esser.

L'informazione rischia così di degenerare in "auto-comunicazione di massa" e il *nudging* politico, reso possibile dalla propaganda ritagliata sul profilo di elettore attribuito all'utente dall'algoritmo, come nel caso *Cambridge Analytica*, rischia di destrutturare dall'interno le dinamiche democratiche.

L'invio di contenuti specificamente ritagliati sulla base del "pedinamento digitale" dell'utente può, infatti, avere una valenza manipolativa del consenso elettorale non paragonabile ad alcun monopolio dell'informazione perché, appunto, capace di adattarsi così perfettamente al pensiero del "bersaglio" da anticiparne il giudizio e limitarne fortemente l'autodeterminazione. Sì che ora, con proiezione nel futuro, incominciamo a discorrere di "neurodiritti".

Peraltro, l'abitudine alle sedicenti "postverità" riduce la notizia a narrazione, sostituendo, nella parresia della rete, i criteri di attendibilità ed esattezza con quelli di mera credibilità e di efficacia narrativa.

La diffusione così rilevante di false notizie è, del resto, alimentata dalla moltiplicazione esponenziale delle fonti d'informazione, non più limitate al giornalismo professionale con il suo sistema di responsabilità e di controlli, ma comprensive di una molteplicità di siti o *blog* dalla natura

più incerta e sottratti, salvo il caso di testate telematiche, alle responsabilità previste in ambito editoriale.

Questa rivoluzione dell'informazione non è neutra dal punto di vista dell'allocazione del potere. Se si erode quella rappresentativa, la democrazia "immediata" ha, infatti, sostituito ai tradizionali corpi intermedi poteri privati capaci di definire, con le condizioni generali di contratto, il perimetro di libertà e di diritti fondamentali, subordinando il tutto alla logica della *lex mercatoria*.

E proprio in un contesto economico fondato sul dato quale risorsa da capitalizzare, questa disciplina rivela un'inattesa attitudine proconcorrenziale. Promuovendo, in particolare - attraverso il principio di trasparenza del trattamento e i limiti posti all'eccessiva concentrazione del potere informativo - le condizioni necessarie per ristabilire la correttezza dei rapporti commerciali e contrastare la formazione di posizioni dominanti quando non addirittura monopolistiche.

L'abuso di posizione dominante contestato dall'Antitrust tedesca a Facebook, per la raccolta di dati da terze parti o le stesse pratiche commerciali "aggressive" imputate al *social network* dalla nostra Agcm, si fondano entrambi su violazioni della disciplina di protezione dei dati. E la ritenuta configurabilità di posizioni dominanti (quali ad esempio quella contestata a Google dalla Commissione Ue), rispetto all'offerta di servizi "*zero-price*", sottende un mutamento di prospettiva importante.

Nella *data economy*, i criteri tradizionalmente utilizzati per ravvisare una posizione dominante, fondati esclusivamente sul prezzo del prodotto, rivelano infatti tutta la loro inadeguatezza. L'ormai netta prevalenza del modello contrattuale servizi contro dati – su cui si basa la solo apparente gratuità dei servizi offerti in rete, - impone di destrutturare le categorie meramente patrimonialistiche su cui si sono rette tanto la disciplina antitrust quanto quella civilistica, se davvero si vuole regolare una realtà che altrimenti rischia di divenire del tutto anomica. La disciplina di protezione dei dati – cui s'ispira la legge tedesca che ha esteso i presidi antitrust a queste ipotesi – rappresenta, in questo senso, lo strumento più adeguato, in quanto consente il governo dell'elemento fondativo della "*zero-price economy*": il dato personale. Che rappresenta, ad un tempo, tanto una risorsa economica (di valore peraltro crescente), quanto l'oggetto di un diritto fondamentale.

Regolarne le condizioni di utilizzo (anche per fini di utilità sociale), l'ambito di circolazione, le garanzie per l'identità che riflette, significa dunque governare il presente e il futuro, armonizzare economia e persona, tecnologia e umanità, sicurezza e libertà.

Non stupisce, quindi, che proprio dalla protezione dei dati abbia preso le mosse il tentativo dell'Unione di affermare la propria sovranità digitale in funzione di tutela dei diritti dei cittadini, attraendo nel raggio di azione della disciplina europea anche i titolari stabiliti al di fuori dei suoi confini, in virtù di un'interpretazione estensiva dei criteri di collegamento sanciti sul punto dalla direttiva.

Questa rivendicazione di un modello europeo di governo del digitale fondato sul primato della persona sta producendo, del resto, effetti conformativi importanti, non solo intra-ordinamentali (la previsione dell'extraterritorialità della disciplina è, ad esempio, mutuata dal Gdpr nel regolamento sul *geoblocking*) ma anche extra-ordinamentali.

Sono infatti sempre più numerosi i Paesi che stanno introducendo discipline di protezione dei dati ispirate al modello europeo, nella direzione - è questo il nostro auspicio- del riconoscimento universale, come fondamentale, del diritto alla protezione dei dati, accanto alla già riconosciuta tutela della vita privata (c.d. *Bruxelles effect*).

2. La disciplina privacy e le sue sfide

Il corso illustrerà i vari aspetti innovativi del nuovo quadro giuridico europeo, soffermandosi su alcuni aspetti essenziali: principi, soggetti, obblighi del titolare, tutele, responsabilità e sanzioni. Si approfondiranno anche alcuni settori particolarmente "sensibili" nei quali la tutela della privacy ha suscitato questioni importanti:

-il lavoro (terreno su cui peraltro la privacy ha assunto, in particolare in Italia, come propria semantica normativa il "codice dell'eguaglianza", tutelando la libertà del lavoratore dalle ingerenze datoriali e così fungendo da fattore di riequilibrio sociale);

-la pubblica amministrazione (settore in cui è stata avvertita con particolare forza l'esigenza di coniugare riservatezza individuale e trasparenza amministrativa, sino alla pronuncia Zanon, n. 20 del 2019 della Consulta);

-il marketing e soprattutto il telemarketing, in cui emerge con sempre maggiore nettezza l'esigenza di valorizzare quel limite della libertà d'iniziativa economica che il Costituente ha ravvisato nella dignità e nella libertà individuale;

- la sanità: àmbito, quest'ultimo, in cui soprattutto durante la pandemia è emersa la necessità di bilanciare esigenze di sanità pubblica e "opacità" della propria sfera privata, tanto più quando siano coinvolte le proprie vulnerabilità, le patologie, le dipendenze, ovvero condizioni che se illegittimamente conosciute possono essere strumentalizzate ed esporre il soggetto a discriminazioni e stigmatizzazioni pericolose.

Se ci soffermiamo ora sulla disciplina sancita dal nuovo quadro giuridico europeo, va anzitutto notato come essa muove dalla consapevolezza della nuova geografia dei poteri, per restituire al cittadino quella capacità di governo dei propri dati indispensabile per riequilibrare, almeno in parte, lo strapotere dei giganti del web. E lo fa tanto nel metodo quanto nel merito.

Anzitutto, sostituendo a uno strumento di armonizzazione quale era la direttiva, uno di uniformazione qual è appunto il regolamento, funzionale alla stessa tutela di questo diritto fondamentale, applicabile anche al di fuori della Ue, in presenza di un'offerta di beni o servizi ai cittadini europei o di un monitoraggio del loro comportamento. A tale fondamentale diritto di libertà si è accordato uno statuto giuridico forte, incentrato sul ruolo di garanzia di Autorità indipendenti e omogeneo nei vari Stati membri.

La tutela, del resto, è estesa non solo sul piano soggettivo ma anche su quello oggettivo: così da comprendere anche i frammenti di informazioni che, combinati con altri, possano rendere identificabile l'interessato o consentirne la profilazione. Ciò che conta nella *data economy* è, del resto, la possibilità di ricondurre un dato non tanto e non solo a una specifica identità, quanto piuttosto ad un profilo, determinando effetti significativi e, spesso, anche potenzialmente discriminatori, in capo agli interessati.

Tutto questo viene perseguito in un quadro che – è importante sottolinearlo - costituisce una nuova sfida per tutti gli operatori coinvolti, a partire dal titolare. Al quale sono riconosciute nuove possibilità di utilizzo dei dati, nell'economia dell'accesso, con un rapporto tra consumatore e impresa molto più dinamico e articolato.

E a fronte di tutto ciò è significativo il rafforzamento dei diritti dell'interessato, con anche implicazioni nuove quali la portabilità dei dati - che consente di ricomporre le tessere del mosaico del nostro io digitale, proteggendo anche la concorrenza da fenomeni di "*lock-in*" - e l'oblio: equilibrio tra storia individuale e memoria collettiva.

Importanti anche i diritti di azione e di opposizione connessi alle decisioni automatizzate sulle quali si basa l'i.a.. Imponendo, infatti, ove se ne ravvisi l'opportunità, la revisione umana del processo decisionale algoritmico, il diritto alla spiegazione della decisione assunta e garanzie particolari per l'uso dell'i.a. nel contesto dei poteri coercitivi e delle indagini di polizia, con il divieto di discriminazioni fondate sui dati sensibili, si sancisce un primo, essenziale statuto normativo dell'i.a. che sta disvelando le sue potenzialità negli ambiti più diversi (si pensi alla valorizzazione che ne ha fatto la giurisprudenza amministrativa rispetto all'algoritmo dei docenti).

Dalla trattazione orientata ai diritti su cui si fonda il Regolamento, deriva poi il passaggio da una tutela in chiave prevalentemente remediale, dunque successiva, a una di tipo essenzialmente preventivo, particolarmente rilevante in ragione del rischio che le garanzie tradizionali di consenso e informativa si relativizzino nel contesto dell'IoT e delle raccolte massive di dati, spesso sfuggenti al controllo individuale per via della frammentazione del processo di gestione del dato, lungo una catena dai molteplici anelli.

Ma l'espressione forse più significativa dell'approccio preventivo concerne la totale responsabilizzazione dei titolari, verso l'adozione di una complessiva strategia aziendale fondata sulla protezione dati, anche considerando che la stessa violazione del principio di responsabilizzazione integra, al pari dell'inottemperanza agli altri principi, gli estremi di un autonomo illecito amministrativo. Su questo aspetto, il corso offrirà spunti di notevole interesse e di particolare ausilio per l'interprete, che risulteranno preziosi anche in sede applicativa.

Altrettanto rilevanti le scelte compiute dal d.lgs. 101 del 2018 che, in sede di adeguamento dell'ordinamento interno al Gdpr, ha tracciato alcuni passaggi importanti. Anzitutto, in linea generale (e nell'esercizio di una delega sostanzialmente conservativa), il decreto ha mantenuto gli istituti della disciplina previgente, non incompatibili con il Regolamento, che hanno dato migliore prova di sé, mutandone la forma ove necessario.

Così per i codici deontologici: espressione del tutto peculiare di un'idea di sussidiarietà normativa orizzontale, di flessibilizzazione della disciplina generale ad opera della fonte auto regolativa, più aderente alle caratteristiche dei trattamenti da regolare e più duttile rispetto all'esigenza di adeguamento all'evoluzione della tecnologia e della società. Nelle materie rimesse agli interventi integrativi degli Stati, pur con la denominazione di regole deontologiche, essi mantengono la loro natura di *soft-law*, costituendo parametri integrativi della legittimità del trattamento.

Addirittura, la loro violazione integra gli estremi di uno specifico illecito amministrativo, che in particolare in materia di giornalismo è auspicabile esplichi efficacia responsabilizzante (ancorché naturalmente non inibitoria della libertà di espressione) rispetto a eccessi che hanno, spesso, deteriorato la qualità dell'informazione.

La sanzione penale, nel rispetto del *ne bis in idem* e del principio di frammentarietà, è riservata a condotte caratterizzate da un disvalore maggiore, lesive della privacy individuale o del corretto esercizio delle funzioni del Garante (quale bene giuridico alla prima strumentale) e pertanto meritevoli della particolare efficacia preventiva di tale sanzione.

Alle elevate sanzioni amministrative pecuniarie si affiancano (in alcuni casi anche in funzione vicaria), le misure "correttive", di natura inibitoria, interdittiva, prescrittiva, sulle quali certamente il corso si soffermerà sottolineandone gli aspetti rilevanti.

Di particolare rilievo è, poi, la scelta discrezionale di imporre, anche per gli uffici giudiziari persino penali, un dpo, nella consapevolezza dell'importanza del contributo che può fornire ai titolari. Da tale figura, del resto, dipende in ogni ambito la "scommessa" dell'*accountability*; la capacità cioè di fare della protezione dei dati non tanto un onere legale da assolvere, quanto un elemento di vantaggio competitivo su cui puntare per reggere alle sfide di una società sempre più fondata sui dati.

Rilevante, peraltro, è la conferma (libera da vincoli europei) delle garanzie per la protezione dei dati anche in un settore, quale quello dell'*intelligence*, tradizionalmente fondata sulla tendenziale prevalenza di un interesse pubblico primario quale la sicurezza nazionale.

Il nuovo quadro giuridico europeo in materia di protezione dei dati rappresenta, dunque, un grande passo avanti nella direzione di un governo equilibrato delle innovazioni tecnologiche che hanno profondamente modificato la nostra società. Ma il successo di questa "scommessa" dipenderà dalla sua tenuta sociale, dalla sua capacità di divenire cioè forma e regola dell'agire dei cittadini, delle amministrazioni, delle imprese. Iniziative come il corso che oggi presentiamo rappresentano, sicuramente, degli ausilii preziosi in questo senso.

3.Cybersecurity e protezione dei dati personali

> La cybersicurezza e la protezione dei dati nelle loro reciproche interrelazioni. E' una suggestione interessante, soprattutto perché riflette su un rapporto tra un interesse di stampo prettamente pubblicistico come, appunto, la *cybersecurity* (trasposizione, sul piano cibernetico, della sicurezza nazionale) e uno, invece, peculiare espressione di quel personalismo sotteso alla nostra Costituzione, com'è la protezione dei dati.

E questa convergenza di individuale e collettivo, di persona e Stato, il loro bilanciamento secondo la gerarchia costituzionale è certamente il fulcro di una democrazia liberale quale è la nostra. Di più: individuale e collettivo, con le loro conseguenti declinazioni (persona e Stato, autonomia e solidarietà, libertà e autorità) sono le componenti costanti intorno alle quali ruota ogni moderna definizione, per mutevole che sia, di Stato di diritto. E lo sono tanto più oggi, in un contesto in cui la crisi della sovranità si riverbera ineludibilmente anche sulla difficoltà di individuazione dell'interesse nazionale, con logiche che riescano a prescindere da nazionalismi, tanto più anacronistici a fronte della progressiva, doverosa integrazione europea.

In questa crisi ha giocato (e tuttora gioca) un ruolo determinante la rivoluzione digitale, con le sue implicazioni e con la sua antropologia, che ha scardinato le coordinate essenziali su cui sinora si sono fondati sistemi istituzionali, relazioni sociali, il sostrato culturale e persino simbolico del nostro vivere. Ne risultano incisi la stessa idea di sovranità e alcune sue prerogative tipiche: il controllo della principale infrastruttura sociale, la disciplina, con le condizioni generali di contratto delle piattaforme; dei modi di esercizio delle libertà; persino lo *jus dicere* tramite giurisdizioni private, divenute arbitri del rapporto tra diritti fondamentali, come avviene per oblio, discorsi ostili, e così via.

Il controllo della rete garantisce, infatti, alle piattaforme un potere di condizionamento che nessun mezzo di comunicazione di massa poteva avere prima, perché privo della capacità di orientare l'opinione pubblica agendo con la formidabile leva del *microtargeting* e della profilazione, così da segmentare l'offerta e proporre non soltanto pubblicità, ma persino informazione mirata e, quindi, più persuasiva.

Questa capacità di condizionamento (*nudging*), propria, in tali termini, soltanto del capitalismo della sorveglianza, può avere effetti determinanti non solo sulle scelte individuali, ma anche su quelle più determinanti per la democrazia, come quelle politico-elettorali.

Come ha dimostrato il caso *Cambridge Analytica*, infatti, con il pedinamento digitale si modella il messaggio politico da promuovere, orientando il consenso elettorale verso il risultato voluto. Si eludono così le garanzie previste da decenni per il pluralismo informativo e politico, come pure per l'autodeterminazione individuale, con il rischio di una manipolazione del consenso, tale da alterare in radice i più rilevanti processi democratici. Ne viene pregiudicata persino l'altrimenti intangibile sovranità statuale, ogniqualvolta la manipolazione del consenso sia organizzata – come parrebbe, a suo tempo, per l'elezione di Trump – da Governi stranieri, così da orientare il risultato elettorale verso la soluzione a loro più favorevole.

E a questa traslazione, sul piano politico, del meccanismo commerciale del *nudging* reagisce, correttamente, l'Europa, con il Regolamento sul *targeting* politico su cui la presidenza del Consiglio e i negoziatori del Parlamento europeo hanno raggiunto un accordo provvisorio proprio il 7 novembre di quest'anno.

Lo statuto paradigmatico della sovranità, quale titolarità di un potere *superiorem non recognoscens* viene così ad affievolirsi a fronte dell'esercizio di queste "autorità di fatto", rischiando di tornare ad essere, con il neofeudalesimo digitale cui allude Joel Kotkin, quella preminenza relativa da cui la modernità l'aveva affrancata. In questa nuova "microfisica" del potere, per riprendere M. Foucault, gioca un ruolo imprescindibile proprio il governo del digitale - complessivamente inteso nelle sue componenti di spazio cibernetico e flussi informativi - attraverso cui si può rideclinare, in forme nuove, l'interesse nazionale.

Se, infatti, una delle più rilevanti insidie alla sovranità muove proprio dal rischio dell'anomia del digitale, di uno spazio virtuale privo di presìdi e regole adeguate, è attraverso la sua *governance* che si può ritessere la trama dell'interesse nazionale.

In questa prospettiva, tanto la *cybersecurity* quanto la protezione dei dati possono svolgere un ruolo dirimente. La prima assicura, infatti, la difesa della frontiera digitale, a cui si indirizzano oggi, perché più vulnerabile di quella fisica, le principali minacce interne ed esterne. I dati sull'incremento esponenziale degli attacchi informatici dopo l'inizio della guerra, anche, per *spillover*, nei confronti dei Paesi non direttamente coinvolti nell'ostilità, sono in questo senso significativi. E', del resto, rilevante che ormai la Nato abbia equiparato gli attacchi *cyber* a qualsiasi altra tipologia di attacco ai fini dell'attivazione della clausola di difesa collettiva.

La protezione dei dati, del resto, svolge un ruolo non meno rilevante sotto due profili. Il primo riguarda le condizioni di libero esercizio dei diritti fondamentali in un contesto sempre più mediato dalle neotecnologie: in quanto presupposto di autodeterminazione e di libertà nel ricorso al digitale, la protezione dei dati assume sempre più i connotati di precondizione per l'esercizio degli altri diritti e delle libertà: un meta-diritto (nel senso suggerito dall'etimo) oltre che un diritto fondamentale, in-somma. E sappiamo che una democrazia liberale si distingue dai regimi autocratici e illiberali proprio per la tutela che accorda ai diritti e alle libertà fondamentali dei cittadini: di qui, dunque, la centralità delle garanzie in una concezione liberale dell'interesse nazionale.

Il secondo profilo di rilevanza della protezione dei dati concerne proprio la sua sinergia con la *cybersecurity*, allorché assicura la tutela di elementi costitutivi dello spazio cibernetico quali, appunto, i dati.

Pertanto, una normativa, come quella di protezione dei dati, che faccia della prevenzione del rischio informatico il suo fulcro essenziale, non può che promuovere le condizioni complessive di protezione indispensabili per la sicurezza cibernetica. La responsabilizzazione dei titolari promossa dal Gdpr, rispetto al rischio "sociale" derivante da sistemi informatici permeabili rappresenta, in questo senso, una risorsa preziosa, non a caso, valorizzata anche dalla normativa in materia di *cybersecurity*: ormai quinta dimensione della sicurezza (assieme a terra, mare, aria, spazio).

Il legislatore europeo ha anzi instaurato una significativa simmetria tra protezione dei dati e sicurezza cibernetica, particolarmente evidente in alcuni istituti (notifica dei *breach;* approccio fondato sul rischio; *privacy e security by design*) che accomunano il Gdpr e le direttive NIS 1 e 2, ma anche il più recente *Cybersecurity Act.*

Tale complementarietà tra protezione dei dati e sicurezza cibernetica non è, del resto, casuale, se si pensa alla funzione originaria della prima nell'ordinamento europeo, considerata un bene giuridico che ciascuno Stato membro avrebbe dovuto tutelare adeguatamente per poter entrare nell'area *Schengen*, in quanto presupposto per la sicurezza dell'area stessa.

Gli sviluppi più recenti dimostrano quanto tale concezione originaria del rapporto tra protezione dei dati e sicurezza – come sinergico, non un gioco a somma zero – fosse lungimirante: in un'economia e in una società fondata sui dati, proteggere questi significa proteggere ad un tempo i singoli e la collettività.

Protezione dei dati come presupposto ineludibile della sicurezza individuale e collettiva, dunque, tanto più necessario al tempo dell'i.a. e del pianeta connesso, in cui ciascun oggetto di uso quotidiano può rappresentare il canale d'ingresso di potenziali attacchi informatici e in cui quindi la superficie di attacco si amplia in progressione geometrica, per effetto dell'estensione esponenziale della connessione. E', del resto, significativo che durante il *summit* Nato a Bruxelles lo scorso anno, l'Alleanza abbia equiparato gli attacchi *cyber* a qualsiasi altra tipologia di attacco ai fini dell'attivazione della procedura di cui all'art. 5. La minaccia *cyber* è entrata dunque, a pieno titolo, tra le sfide sistemiche (lo ha ricordato il Capo dello Stato il 4 novembre scorso) e la protezione dei dati concorre a un'organica strategia di difesa.

Ed è proprio sulla sinergia tra *cybersecurity* e protezione dei dati che può fondarsi una nuova declinazione dell'interesse nazionale, inclusiva anche della componente strategica che è oggi la sovranità digitale.

Di questa nozione si possono, ovviamente, dare varie letture. Ve n'è una più minimalista, ma anche pragmatica, che enfatizza l'esigenza di indipendenza nazionale nella fornitura, gestione e finanche negli stessi assetti proprietari delle infrastrutture tecnologiche. È il tema che ricorre spesso a fronte dei casi di acquisizione, da parte di aziende straniere, del controllo societario rispetto ad *asset* strategici e che si è posto, di recente, con il caso Kaspersky. E' certamente ineludibile (la guerra lo ha chiarito ulteriormente) la disponibilità esclusiva, da parte di ciascun Paese o area (come per l'UE) di proprie infrastrutture tecnologiche almeno in settori strategici, tali da spezzare quella dipendenza - non soltanto funzionale - da fornitori stranieri, della cui opportunità è lecito dubitare.

Questa declinazione "materialistica" della sovranità nazionale coglie, senza dubbio, la rilevanza del rapporto tra l'assetto dominicale delle tecnologie e la loro funzionalità anche in termini democratici, sottolineando l'esigenza di una *governance* non soltanto interna (non straniera) ma, soprattutto, pubblica delle principali infrastrutture digitali.

Ma, accanto a questa, vi è una diversa accezione di sovranità digitale, declinata in chiave valoriale, alludendo cioè a quella disciplina del rapporto tra diritto, persona e tecnica che finisce sempre più con il definire il profilo identitario di un ordinamento, sotto il profilo sociale, culturale, giuridico, persino politico. In questo senso, sovranità digitale vuol dire governo della tecnica secondo la gerarchia assiologica espressa da ciascun ordinamento, conformemente alla sua identità e tradizione costituzionale. E' significativo che l'UE abbia ritrovato, in particolare sul terreno del governo antropocentrico della tecnica, un'unità smarrita da tempo in molti altri settori, riaffermando la propria identità come ordinamento fondato su alcuni, irrinunciabili, valori.

Nel raffronto con gli Usa sul terreno della disciplina della *privacy* è emersa con chiarezza quest'accezione identitaria della sovranità digitale e dello stesso interesse (qui sovra-) nazionale: la Corte di Giustizia europea ha, soprattutto in questi casi, contributo a delineare l'Ue come "comunità di diritto" caratterizzata da un non derogabile sistema di tutela della persona (anche e soprattutto rispetto alle insidie poste dalle nuove tecnologie).

Nelle due sentenze *Schrems*, la Corte sottende un'idea di sovranità digitale come non subalternità del sistema europeo di tutela (anche e soprattutto) della privacy rispetto ad ordinamenti, come quelli americani, meno garantisti e capaci dunque di neutralizzare le tutele accordate dal diritto europeo ogniqualvolta i dati, nella loro inevitabile mobilità transnazionale, siano trasferiti negli Usa.

In questo senso, dunque, l'affermazione della sovranità digitale europea, lungi da pretese egemoniche o autarchiche, è invece come rivendicazione di un sistema di tutele che connota l'Unione come spazio di libertà e diritti, capace di assicurare un governo antropocentrico e personalista dell'innovazione. Sul terreno della *cybersecurity* si assiste a un percorso affine, attraverso la progressiva armonizzazione delle discipline, ritenute strategiche per la difesa di una frontiera, quale quella digitale, ormai non più soltanto nazionale.

Proprio dalla protezione dati e dalla *cybersecurity* può derivare, allora, la spinta a ripensare l'interesse nazionale tenendo conto delle esigenze di sovranità digitale. Nozione da declinare, però, all'interno di quel sistema di valori e obiettivi che caratterizza la "Comunità di diritto" cui l'Italia ha scelto di appartenere: l'Unione europea, che pone – come recita il preambolo della Carta di Nizza – la persona al centro della sua azione.