La cybesecurity è strategica per i diritti del cittadino e per la difesa del Paese

Il ruolo dell'Agenzia per la cybersicurezza

Bruno Frattasi, Oreste Pollicino, Flavia Scarpellini

Nel volgere degli ultimi anni, la cybersicurezza e le questioni che in modo sempre più sistemico fa emergere per la tenuta - tra le altre cose anche dello stato di diritto - si sono poste progressivamente al centro dell'attenzione generale, andando ben oltre la dimensione di nicchia per specialisti che ne ha caratterizzato i primi passi. E ciò sia dal punto di vista dell'interesse della dottrina – specialmente per quanto riguarda le implicazioni istituzionali – che per la stessa giurisprudenza ed europeo. Parlare di trasfigurazione a proposito del mutamento di ruolo della cybersicurezza sarebbe forse eccessivo. Ci pare però si possa legittimamente parlare di un importante passaggio trasformativo. Anzi, un doppio passaggio.

In primo luogo, non è più (soltanto) una questione tecnica per la difesa della sicurezza nazionale (dove gli Stati difendono la propria sovranità e acquisiscono informazioni sugli altri Stati in funzione preventiva e di *intelligence*), ma è una priorità strategica per le imprese (minacciate dal furto delle informazioni da parte di concorrenti, dipendenti infedeli e ricattatori) a difesa dei propri interessi economici e del rapporto fiduciario con gli utenti che devono, per l'appunto, potersi fidare di chi riceve e gestisce i loro dati.

In secondo luogo, la cybersicurezza ambisce sempre più ragionevolmente a essere parte della costellazione dei diritti fondamentali rilevanti nel contesto digitale. È evidente, in particolare, il collegamento e la progressiva emancipazione dalla tutela dei dati personali. Per un lungo periodo, la legislazione sulla privacy (da ultimo il Gdpr) ha richiesto, in modo rigoroso, la difesa cibernetica delle libertà personali nell'ambito del trattamento dei dati personali, trattandola come un unicum. In effetti, per alcuni anni la cybersicurezza è stata percepita, da un punto di vista civilistico, come una «sotto specie» del diritto alla *privacy*. Oggi è venuto il tempo di attribuire una autonomia concettuale e assiologica al diritto alla cybersicurezza. Un diritto che si è ulteriormente evoluto insieme all'uso della tecnologia, sino alla difesa dei valori di libertà: dalle campagne elettorali condotte via web e distorte con l'uso di *fake news*, sino alla protezione della nostra «personalità digitale».

Quest'ultima frontiera pone nuovi interrogativi giuridici, soprattutto di natura costituzionale, per gli inediti rapporti tra tecnologia, sovranità nazionale, diritti dei cittadini e ruolo dei grandi *players* del mondo digitale. Richiede anche la necessità di un cambio di approccio: ferma restando la lotta alla criminalità e la costruzione di un sistema tecnologico sicuro e affidabile, occorre alimentare un clima di collaborazione tra tutti gli *stakeholders*, dove ognuno «faccia la sua parte» per assicurare che la tecnologia mantenga la sua neutralità e si ponga al servizio del progresso.

In tal contesto, la *cybersecurity* si sta ponendo, nel recente dibattitto, sempre più – lo si accennava prima – come un diritto fondamentale della persona, dotato di una sua autonomia assiologica-concettuale. Tale autonomia si estrinseca intanto nel rapporto tra individui e poteri pubblici, laddove essa si configura come diritto di libertà, in una forma non dissimile dal diritto alla sicurezza che i cittadini possono esigere di vedere garantita sul piano della realtà fisica.

Allo stesso tempo, l'autonomia concettuale di cui si parla si estrinseca anche nel confronto tra l'individuo e i giganti del Tec, laddove, soprattutto per merito del legislatore europeo, la posizione del singolo è venuta a rafforzarsi e ad acquisire un minore livello di soggezione rispetto ai poteri privati, rappresentati, appunto, dai grandi gruppi tecnologici.

Il legislatore nazionale e, ancor prima, quello euro unitario hanno ben compreso queste problematiche e hanno adottato una serie di provvedimenti volti a contrastare i rischi che si sono fin qui evocati.

Non vi è ancora un riconoscimento del diritto alla *cybersecurity*, inteso come autonoma posizione sostanziale della persona. Tuttavia, un cambiamento di approccio è già presente, anche in ambito nazionale, in considerazione dell'ampliarsi del numero dei soggetti destinatari della disciplina rilevante in materia di cybersicurezza, la cui piena attuazione ridonda nella tutela del cittadino dalla minaccia alla sua libertà nella dimensione digitale, dando seguito, anche in quest'ultima dimensione, a una concezione prismatica della sicurezza da tempo evidenziata nel dibattito pubblico.

In questa direzione, le misure che entreranno a regime nei prossimi mesi (le direttive 2555/2022 – c.d. Nis2 - e 2022/2557- c.d. Cer, nonché, per il settore finanziario, il Regolamento 2022/2554 - c.d. Dora) interesseranno sempre più ampi settori dell'economia e delle istituzioni. Si calcola che saranno circa 50mila le imprese in Italia interessate dalla Nis2. Inoltre, la recente disciplina nazionale di cui alla L. 90/2024 ha già esteso talune misure di *cybersecurity* anche a nuovi settori della Pa, sia centrali che locali, e relative società *in house*. Ciò in aggiunta ai soggetti (in parte coincidenti) di cui al Perimetro di Sicurezza Nazionale Cibernetica che è già operativo.

In tale paradigma, uno dei maggiori protagonisti del cambiamento (anche di approccio) è l'Agenzia per la Cybersicurezza Nazionale (Acn). Ad esempio, la L. 90/2024 ed il decreto legislativo di recepimento della direttiva Nis2 prevedono che l'Acn svolga già un innovativo compito di «guida e di «supporto» alle imprese destinatarie, fermo restando il ruolo «educativo» e di «promozione» della cultura in materia di sicurezza cibernetica, nonché di catalizzatore (anche con i centri di ricerca e le Università) dell'innovazione e delle buone prassi (unitamente alle altre istituzioni a ciò preposte) che è già nella sua *mission*. Parallelamente, gli operatori saranno chiamati a farsi parte diligente sia tramite l'effettuazione di tempestive notifiche alle autorità degli attacchi *hacker*, sia registrandosi in modo proattivo (ritenendosi destinatari della Nis2) sulla piattaforma digitale che verrà allestita dall'Acn.

La moltiplicazione della normativa (nazionale e comunitaria) è spesso, aggiungeremmo erroneamente, percepita dagli operatori come solo afflittiva, anche per le rilevanti sanzioni amministrative ivi previste. Si parla, infatti, spesso di *compliance* e di «evitare sanzioni e responsabilità» (oggi i Consigli di amministrazione sono in prima linea per la normativa comunitaria – es. Nis2 e Dora - che richiede una «*governance* della cybersicurezza» non demandabile a terzi).

Con la trasformazione che si è evocata rispetto al ruolo della *cybersecurity*, è necessario anche provare a utilizzare un linguaggio, con riguardo all'Agenzia, che valorizzi, come si diceva, il suo ruolo promozionale ed eviti riferimenti devianti ad una presunta funzione, in senso lato, «repressiva».

Direttore generale dell'Agenzia per la cybersicurezza nazionale; professore di Diritto costituzionale all'Università Bocconi di Milano; avvocato per la governance societaria della cybersicurezza

L'ORGANISMO HA UN RUOLO DI GUIDA E DI SUPPORTO ALLE IMPRESE OLTRE A QUELLO DI EDUCAZIONE E PROMOZIONE

TIMOTHY A. CLARY / AFP

Fuori dall'ombra. La cybersicurezza come diritto fondamentale