INTERVENTO DEL PRESIDENTE DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, ANTONELLO SORO

"Spazio cibernetico bene comune: protezione dei dati, sicurezza nazionale" - convegno organizzato dal Garante per la privacy il 30 gennaio 2020

La sicurezza della dimensione cibernetica è costantemente esposta a minacce : minacce sempre più "ibride", tali da configurare una sorta di cyber guerriglia permanente.

Nel 2019 il cybercrime è cresciuto del 17% a livello mondiale rispetto alle cifre del 2018: anno già definito, per quel che riguarda l'Italia, il peggiore per la sicurezza cibernetica.

Gli esperti hanno tracciato preoccupanti previsioni sui possibili rischi e sulle tendenze per il 2020, delineando uno scenario fatto di attacchi sempre più sofisticati.

Nei mesi scorsi, la Polizia Postale ha portato alla luce quello che parrebbe configurarsi come il più grave attacco alle banche dati istituzionali finora realizzato, con tecniche di phishing che consentivano l'accesso a sistemi informativi tra i più rilevanti per il Paese, dai quali estrarre dati da rivendere ad agenzie investigative e di recupero crediti.

Ma gli attacchi informatici sono divenuti anche mezzi d'ingegneria bellica.

Basta pensare ai recenti avvenimenti in Medio Oriente, anticipazione di quel che sarà il paradigma dello scontro militare nei prossimi anni: droni armati e attacchi informatici utilizzati quali vere e proprie armi, dotate di una potenza straordinariamente maggiore.

Quella cibernetica è dunque la dimensione su cui si sposta sempre più la dinamica dei conflitti, palesi o latenti, tra Stati e tra soggetti, operata attraverso dati e sistemi informativi.

Ed è, peraltro, è l'unica dimensione della sicurezza e della difesa sostanzialmente priva di un'adeguata cornice di diritto internazionale.

Un'efficace strategia di prevenzione dei rischi cibernetici presuppone quindi, anzitutto, la consapevolezza dei fattori su cui si basano, rispettivamente, azione e reazione: la tecnologia e il diritto.

Se, infatti, le nuove tecnologie sono il presupposto essenziale della 'potenza geometrica' delle nuove minacce, il diritto è l'unica risorsa capace di mettere la tecnica al servizio dell'uomo, della libertà, della sicurezza.

E, anzi, un'alleanza di tecnologia e diritto può rappresentare l'architrave di una risposta democratica e lungimirante alle nuove minacce del digitale, inevitabilmente connesse agli opposti, straordinari benefici.

Questo presuppone anzitutto il massimo equilibrio tra le discipline deputate a governare il rapporto tra le libertà e il lato oscuro della tecnica , ovvero quella di protezione dati e quella a tutela della sicurezza cibernetica.

Tra le quali intercorre un rapporto indubbiamente complesso, ma che tra antagonismi e inattese sinergie, dice moltissimo di una società in cui l'esibizione incontenibile della vita privata riflette una crisi profonda di fiducia e coesione sociale: elementi - questi - su cui in passato si fondava un'assai diversa percezione tanto della sicurezza quanto della libertà.

Da un lato, infatti, la tutela della sicurezza cibernetica (quinta, ma sempre più rilevante dimensione della sicurezza nazionale), ha legittimato limitazioni incisive della privacy, in nome del contrasto a minacce tanto immanenti quanto pulviscolari, con il ricorso a strumenti investigativi spesso di tipo massivo.

Social e signal intelligence, sorveglianza strategica (e non più solo "mirata"), data mining: sono solo alcune delle forme che può assumere l'azione di prevenzione e che estende il suo raggio di azione quanto più la società iperconnessa alimenta continui flussi informativi.

La potenza della tecnologia, da un lato, e le caratteristiche della minaccia cibernetica (acefala, mutevole, nebulosa) dall'altro, ampliano dunque, inevitabilmente, lo spettro dell'azione investigativa.

Questo ha implicazioni importanti sotto il profilo delle libertà e degli equilibri democratici.

Se pensiamo che- nel nostro Paese- i gestori conservano, ogni giorno, circa 5 miliardi di tabulati di traffico telefonico e telematico per fini di contrasto, dobbiamo chiederci anzitutto se nell'ambito di una massa così enorme di dati sia davvero possibile rinvenire quelli utili; se, insomma, estendendo così a dismisura il pagliaio sia ancora ragionevole pensare di poter trovare l'ago.

E un'azione di contrasto così penetrante determina una limitazione della privacy che sarà legittima solo se e in quanto strettamente conforme al principio di proporzionalità, su cui la Corte di giustizia ha costruito l'architrave del rapporto tra prevenzione e libertà.

Ma, circoscritte le politiche di sicurezza e i poteri degli organi di contrasto entro il perimetro della proporzionalità, sarà chiaro come quello tra protezione dati e cyber security non sia un gioco a somma zero ma, anzi, un rapporto fatto di sinergie e reciproche funzionalità.

L'esperienza del protocollo d'intenti con il Dis è, in questo senso, emblematica.

Esso, infatti, è stato siglato proprio quando, nel 2013, è emersa l'esigenza di un parallelismo tra estensione dei poteri degli Organismi e corrispondente aggiornamento delle funzioni di garanzia dell'Autorità.

Nato, dunque, per bilanciare esigenze di sicurezza e protezione dei dati, tale strumento innovativo ha dimostrato come questi beni giuridici essenziali, tutt'altro che necessariamente antagonisti, siano invece assai più complementari di quanto si possa immaginare.

E questo perché la cyber security implica anzitutto, inevitabilmente, la protezione dei dati e delle infrastrutture di cui è composto l'ecosistema digitale.

E' significativo che, a seguito della direttiva NIS e del Gdpr, il protocollo sia stato integrato, prevedendo la comunicazione, da parte del Garante ai Servizi, dei data breach suscettibili di rilevare per la sicurezza nazionale.

Del resto, una normativa che fa della tutela dei dati e dei sistemi dal rischio informatico il suo fulcro essenziale, non può che promuovere quelle condizioni complessive di resilienza indispensabili per la sicurezza cibernetica.

La responsabilizzazione dei titolari promossa dal Regolamento, rispetto al rischio "sociale" derivante da sistemi informatici permeabili è, in questo senso, una risorsa preziosa.

Il legislatore europeo ha anzi instaurato una significativa simmetria tra protezione dati e sicurezza cibernetica, particolarmente evidente in alcuni istituti che accomunano il Regolamento, la direttiva NIS e lo stesso regolamento 2019/881 sulla cybersecurity.

Tale complementarietà tra protezione 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 garantire per poter entrare nell'area Schengen, in quanto presupposto per la sua sicurezza.

Gli sviluppi più recenti dimostrano quanto lungimirante fosse tale concezione del rapporto tra protezione dati e sicurezza: in un'economia e una società fondata sui dati, proteggere questi significa tutelare ad un tempo i singoli e la collettività.

Protezione dati come presupposto ineludibile della sicurezza individuale e collettiva, dunque, tanto più necessario all'epoca dei big data e dell'Internet "di ogni cosa".

In tale contesto, in cui ciascun oggetto di uso quotidiano può rappresentare il canale d'ingresso di potenziali attacchi informatici e in cui quindi le fonti di rischio si moltiplicano a dismisura, è indispensabile fare della protezione dei dati, dei sistemi e delle infrastrutture l'obiettivo prioritario delle politiche pubbliche, perché da questo dipende la tutela della persona ma anche la sicurezza nazionale.

La crescente complessità dei sistemi genera, infatti, vulnerabilità sfruttate per attacchi informatici che possono paralizzare reti di servizi pubblici essenziali, canali di comunicazione istituzionali di primaria importanza, con un impatto, dunque, concretissimo sulla vita pubblica.

Le caratteristiche delle minacce, come per il terrorismo, non sono più prevedibili in quanto pulviscolari e in continua evoluzione.

La difesa diviene così asimmetrica anche perché le catene, più complesse, su cui si articolano i flussi informativi presentano una molteplicità crescente di anelli deboli.

Ciò evidenzia come le sinergie che caratterizzano il rapporto tra protezione dati e cyber security non siano soltanto normative ma attengono a un livello più profondo e strutturale, perché tendono entrambe alla protezione della realtà digitale, dei dati e i sistemi considerati non isolatamente, ma nelle loro reciproche inferenze.

La sicurezza cibernetica è stata, del resto, definita bene comune, la cui tutela avvantaggia tutti, proprio perché attiene a una realtà, quale quella digitale, fondata sull'interdipendenza di dati, sistemi, soggetti.

In tale prospettiva abbiamo orientato la nostra azione in questi anni, rilevando anzitutto l'esigenza di razionalizzare il patrimonio informativo, soprattutto pubblico, per ridurre la superficie d'attacco da cui estrarre dati spesso utilizzati a fini di spionaggio.

Abbiamo poi sottolineato le implicazioni dovute alla sempre più frequente esternalizzazione a privati di segmenti importanti dell'attività amministrativa o, ancor più, investigativa, che ne rendono alquanto più permeabile la filiera.

Ricordo, in tal senso, la significativa attività svolta nel 2014 rispetto ai nodi di interscambio internet (ixp), gestiti da privati non sempre in modo adeguato e dalla cui sicurezza dipendono, tra l'altro, la sicurezza nazionale, l'efficacia delle indagini, l'incolumità dei singoli.

Come, del resto, dimostrano i casi Hacking Team ed Exodus, la vulnerabilità dei sistemi utilizzati dai privati incaricati e la negligenza frequente nell'osservanza degli obblighi di protezione espone a un rischio insostenibile non solo la riservatezza dei cittadini, ma anche i dati investigativi e spesso persino la sicurezza nazionale.

Solo l'adozione di misure adeguate, da parte di ciascun soggetto coinvolto in ogni fase dell'attività captativa, può dunque contribuire a minimizzare i rischi connessi alla frammentazione dei centri di responsabilità, derivanti dal coinvolgimento di soggetti diversi nella "catena" delle attività investigative.

E la stretta dipendenza della sicurezza della rete da chi ne gestisca i vari snodi e "canali" pone il tema della sovranità digitale, da declinarsi non in chiave nazionalistico-autarchica, quanto piuttosto investendo, nella governance della dimensione digitale, la propria identità giuridica e politica.

E poiché le minacce sono globali, credo che l'obiettivo debba essere la complessiva assunzione di responsabilità pubblica rispetto a un interesse, quale la sicurezza cibernetica, da cui dipende in primo luogo l'indipendenza dei Paesi e che deve sempre più declinarsi in chiave sovranazionale, spostando, proprio come è stato per la protezione dati, il proprio orizzonte sulla dimensione (almeno) europea.

Di fronte a minacce che vanno dalla guerra cibernetica all'antagonismo politico digitale, dunque, le politiche pubbliche devono mettere al centro il valore della protezione dati quale condizione di competitività, sicurezza e assieme di libertà, per non soggiacere alla spinta neocolonialista delle autocrazie digitali.

Non a caso, l'Europa ha reso la protezione dati un fattore identitario, ritrovandovi, proprio in un momento in cui riaffiorano le spinte divisive, quell'aspirazione federale così ostacolata in altri campi e tale da segnare un vero e proprio divario transatlantico nella gestione del rapporto tra tecnica e diritti, economia e libertà.

E questa vocazione unitaria (ma anche, appunto, identitaria), superando i particolarismi che spesso privano il diritto del suo necessario 'sguardo lungo', ha consentito a questa disciplina di divenire il fronte più avanzato di governance del digitale, una vera e propria costituzione per l'algoritmo, a cui poi molte altre normative (anche extraeuropee) hanno attinto.

La forza attrattiva e la vocazione "costituzionale" della protezione dati si fondano, del resto, sulla lungimiranza di alcuni suoi istituti essenziali.

Si pensi all'affermazione – pressoché unica nel panorama giuridico attuale e capace di offrire tutela in ogni campo– del diritto alla non esclusività e non discriminatorietà della decisione algoritmica, che non deve insomma divenire parametro unico né tantomeno distorsivo di valutazione della persona.

Le implicazioni di ordine giuridico-costituzionale, politico-economico, persino etico di questa previsione sono determinanti e, se forse non risolutive, certamente ineludibili in una società sempre più fondata sul potere dell'algoritmo.

Inoltre, la prevista "extraterritorialità" del Regolamento – che si applica anche a titolari extra-Ue per il fatto di trattare dati di quanti si "trovino" in Europa – ha implicazioni dirompenti sotto il profilo giuridico, economico, simbolico.

Non solo, infatti, ciò consente di attrarre nel diritto europeo i giganti del web, sfuggenti a ogni altro tentativo di regolazione, assicurando a chiunque si trovi in Europa (non solo ai "cittadini", come doveroso per un diritto fondamentale) un paniere di diritti non derogabile in ragione della sede, più o meno di comodo, dell'attività aziendale.

Tale previsione afferma, con tutta la forza della regola che è insieme principio, che in uno spazio defisicizzato come la rete la sovranità vada declinata in forme nuove, meno legate al tradizionale criterio di territorialità e più attente, invece, alla capacità degli Stati di rendere effettiva la tutela dei diritti e la stessa forma democratica, di fronte a sempre nuove spinte illiberali.

Sono significativi, in tal senso, i rischi cui un uso manipolativo dei dati personali, anche da parte di potenze estere, può avere sulla sovranità nazionale e sulle scelte politiche essenziali che ne determinano l'esercizio.

La vicenda Cambridge Analytica ha dimostrato, infatti, come il microtargeting basato sulla profilazione dei cittadini e la conseguente propaganda elettorale, mirata in base al tipo di elettore stilato dall'algoritmo, determini un pesante condizionamento del processo di formazione del consenso, che può essere gestito da potenze straniere per orientare a loro favore il risultato elettorale.

Non a caso, a seguito della vicenda Cambridge Analytica, il Congresso Usa ha iniziato a discutere un disegno di legge federale per la protezione dati modellato sul paradigma europeo e la California ha approvato una normativa in tal senso.

E' infatti apparso evidente come il contrasto dello sfruttamento dei dati personali in funzione distorsiva del consenso elettorale sia funzionale, anche, alla difesa della sovranità nazionale, in un contesto di progressiva proiezione del conflitto e del potere sul dato e su quella potentissima infrastruttura sociale che è la rete.

La stessa competizione per l'egemonia tecnologica cela, oggi, una più stretta connessione con le dinamiche geopolitiche, suscettibile di coinvolgere in maniera determinante profili di sicurezza nazionale.

Condivisibile, quindi, la preoccupazione, espressa dal Copasir, per la possibile recessività delle esigenze di cyber security rispetto agli interessi commerciali, che coglie fino in fondo le implicazioni proprie di un certo tipo di neo-imperialismo digitale.

Come sottolineato dal Consiglio Ue, tra i fattori di rischio correlati al 5 G vanno infatti annoverati non solo i profili tecnologici, ma anche quelli ordinamentali.

Ciò impone, dunque, di considerare i rischi connessi alla fornitura di tecnologia da parte di aziende, quali quelle cinesi, inserite in un contesto di dirigismo (anche) economico che le obbliga a cooperare con il Governo, fornendogli pezzi importanti del proprio patrimonio informativo, con implicazioni da non sottovalutare sul piano della sicurezza nazionale.

In tale prospettiva abbiamo, peraltro, in più occasioni auspicato un "Privacy Shield" con la Cina, per garantire il rispetto di alcune basilari condizioni di tutela del diritto alla protezione dei dati (se non altro) dei cittadini europei.

Siamo consapevoli che un simile accordo necessiterebbe di una revisione radicale del sistema giuridico cinese, tale da escludere, in particolare, il prelievo sostanzialmente illimitato, da parte del Governo, dei dati nella disponibilità delle aziende.

E tuttavia la dimensione e l'incombenza dei rischi per la sicurezza dei nostri paesi non consentono né inerzia né, tantomeno, rassegnazione.

E in questa competizione sino-americana per l'egemonia sulla potenza di calcolo, l'Europa rischia di perdere ogni possibile ruolo, se non ha la forza di opporre, al dumping digitale, un'idea di innovazione democraticamente sostenibile, fondata su principi di trasparenza e responsabilità algoritmica e tale da coniugare economia e diritti, libertà e sicurezza.

Che tornerebbero ad essere valori complementari e non antagonisti, quali del resto l'ordinamento europeo li delinea, nella consapevolezza di come la democrazia viva necessariamente di entrambi.

Sarà forse necessario aggiornare l'agenda politica, mettendo al centro idee e progetti per governare la società digitale nei prossimi anni, per garantire i diritti e le libertà in questa nuova dimensione della vita: la protezione dati può essere, in questa prospettiva, una bussola affidabile.