Tecnologia e diritto devono allearsi per una corretta governance digitale - Intervista ad Antonello Soro

Tecnologia e diritto devono allearsi per una corretta governance digitale

Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali
(Di Massimiliano Cannata, Cybersecurity trends, 16 aprile 2020)

"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 un orizzonte fatto di attacchi sempre più sofisticati".

Presidente Soro questo il messaggio che è arrivato dalla 14° giornata europea dedicata alla protezione dei dati personali. A quali scenari dobbiamo preparaci?

La sicurezza della dimensione cibernetica è costantemente esposta a minacce sempre più "ibride", tali da configurare una sorta di cyber guerriglia permanente. 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. E' un fatto emblematico che la dice lunga sui trend evolutivi di un fenomeno come quello del cybercrimine che richiede, per poter essere arginato, competenza, tempestività e immediata capacità di risposta.

Questo numero di Cybersecurity Trends è dedicato al rapporto tra Cyber Security e geopolitica. Come vede questo delicato binomio?

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 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. Per altro stiamo parlando dell'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, infatti, la consapevolezza dei fattori su cui si basano, rispettivamente, azione e reazione: la tecnologia e il diritto.

Il diritto deve essere al servizio dell'uomo, ma troppo spesso ce ne dimentichiamo...

Il diritto è l'unica risorsa capace di mettere la tecnica al servizio dell'uomo, della libertà, della sicurezza. Sarebbe per altro auspicabile un'alleanza tra tecnologia e diritto che può rappresentare l'architrave di una risposta democratica e lungimirante alle nuove minacce del digitale, minacce fortunatamente controbilanciate dalle straordinarie potenzialità di questi mezzi. 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.

E' corretto definire la cyber security come l'altra faccia della Privacy, come ha ricordato introducendo il dibattito Arturo di Corinto?

Tra protezione dei dati e tutela della sicurezza informatica 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. Occorre ricordare a questo proposito che la tutela della sicurezza cibernetica 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, data mining: sono solo alcune delle forme che può assumere l'azione di prevenzione, che estende il suo raggio di intervento quanto più la società iperconnessa alimenta continui flussi informativi.

Al rapporto tra democrazia e potere dei dati ha dedicato un interessante saggio (Libertà algoritmi e umanesimo digitale, ed. Baldini e Castoldi n.d.r.). Sotto il profilo degli equilibri demo-cratici, come va bilanciato il rapporto tra sicurezza e tutela della privacy?

La potenza della tecnologia e le caratteristiche della minaccia cibernetica sempre più evoluta implicano un aumento dello spettro dell'azione investigativa. Questo, come giustamente lei sottolinea nella domanda, non può che avere degli effetti sotto il profilo delle libertà e degli equilibri democratici. Dobbiamo pensare che, nel nostro Paese, i gestori conservano, ogni giorno, circa 5 miliardi di tabulati di traffico telefonico e telematico per fini di contrasto, nell'ambito di una massa così enorme di dati non è certo facile rinvenire quelli utili. Detto in altri termini: se stendendo così a dismisura il pagliaio può ancora essere ragionevole pensare di poter trovare l'ago?

La collaborazione dell'Autorità Garante con il DIS (Sistema di informazione per la sicurezza della repubblica n.d.r) è un punto certamente qualificante sul fronte della protezione dei dati. Può spiegare in che senso?

Il protocollo d'intenti siglato con il Dis nel 2013, è stato dettato dalla precisa esigenza di definire un parallelismo tra un'estensione dei poteri degli Organismi e un adeguato corrispondente aggiornamento delle funzioni di garanzia dell'Autorità. A dimostrazione della delicatezza del problema anche il legislatore europeo si è mosso, instaurando una significativa simmetria tra protezione dati e sicurezza cibernetica, che appare evidente nella definizione di alcuni istituti che accomunano il Regolamento, la direttiva NIS e lo stesso regolamento 2019/881 sulla cybersecurity.

Dal suo intervento è emerso in maniera netta come la cyber security debba essere considerata come un diritto dell'uomo nella società delle reti, in quanto sfera che chiama in causa i diritti inviolabili di espressione, movimento, partecipazione, relazione. E' una interpretazione corretta?

E' corretta se si considera che in un'economia e una società fondata sui dati, proteggere questi significa tutelare ad un tempo i singoli e la collettività. Nel contesto della società digitale 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, molto forte sulla vita pubblica. Nel "capitalismo della sorveglianza", in particolare, i rischi sono ancora più alti se pensiamo che le minacce, come nel caso del terrorismo, non sono più prevedibili avendo un carattere "pulviscolare" 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.

In questa prospettiva lo spazio cibernetico diventa bene comune, tema molto caro a Stefano Rodata. Cosa vuoi dire in concreto?

Le sinergie che caratterizzano il rapporto tra protezione dati e cyber security, per quanto ho cercato di spiegare in questa conversazione, non sono soltanto normative ma attengono a un livello più profondo e strutturale, perché tendono entrambe alla protezione della realtà digitale, dei dati e i dei sistemi considerati non isolatamente, ma nelle loro reciproche inferenze. Per questa ragione la sicurezza cibernetica è stata definita bene comune, la cui tutela avvantaggia tutti, proprio perché attiene a una realtà, quale quella digitale, fondata sull'interdipendenza di dati, sistemi, soggetti.

L'intelligence geopolitica dei dati e la spinta verso l'egemonia tecnologica, che molti stati hanno messo in atto può determinare un mutamento degli equilibri politici ed economici a livello mondiale?

La domanda è complessa e implica più livelli di analisi. Rimanendo al tema di questa intervista occorre sottolineare come la stretta dipendenza della sicurezza della rete da chi ne gestisca i vari snodi e "canali" stia di fatto facendo emergere il tema della "sovranità

digitale'; da declinarsi non in chiave nazionalistico-autarchica, quanto piuttosto nell'ottica di una governance della dimensione digitale, che oggi esprime un'identità giuridica e politica. Detto in sintesi: dal momento che 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 su una prospettiva quanto meno europea.

Il politologo francese Bertrand Badie in un celebre saggio parla di fine dei tenitori e del declino del "Leviatano" di Hobbes. In maniera, per certi aspetti imprevedibile, non Le pare che si stia facendo strada, insieme all'orizzonte di una diversa concezione della sovranità, cui lei faceva prima cenno, il pericolo di un "neoimperialismo digitale" fondato sul controllo dei dati e delle informazioni?

In uno spazio "defisicizzato" come la rete la sovranità va 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, per citare un caso sicuramente eclatante, ha dimostrato come il cosiddetto "microtargeting" basato sulla profilazione dei cittadini e la conseguente propaganda elettorale, mirata in base al tipo di elettore stilato dall'algoritmo, possa determinare un pesante condizionamento del processo di formazione del consenso, che risulta gestibile da potenze straniere per orientare a loro favore il risultato elettorale. Sta accadendo che la competizione sempre più forte per l'egemonia tecnologica cela, oggi, una più stretta connessione con le dinamiche geopolitiche, suscettibile di coinvolgere in maniera determinante profili di sicurezza nazionale. Il rischio di un "neo imperialismo digitale" cui lei faceva riferimento è stato colto ed evidenziato dalla preoccupazione espressa dal Copasir a fronte di quella che appare come un'evidente debolezza delle legittime esigenze di cyber security, sempre più sopravanzate dalla forza schiacciante di interessi commerciali che la fanno da padrone, limitando di fatto la libertà degli utenti e persino l'esercizio della sovranità da parte degli stati nazionali.

L'Europa, nella complessa partita di una governance globale del digitale?

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, tale da segnare un vero e proprio divario transatlantico nella gestione del rapporto tra tecnica e diritti, economia e libertà. Questa vocazione unitaria, che purtroppo spesso latita in altri ambiti, ha permesso di superare i particolarismi che spesso privano il diritto del suo necessario "sguardo lungo", ha consentendo a questa disciplina di divenire il fronte più avanzato di una governance del digitale, in grado di spingersi verso una vera e propria costituzione per l'algoritmo, a cui poi molte altre normative (anche extraeuropee) hanno attinto. In prospettiva penso che si renderà quanto mai necessario aggiornare l'agenda politica, mettendo al centro idee e progetti per governare la società digitale, al fine di garantire i diritti e le libertà in questa nuova dimensione della vita rispetto a cui la protezione dati è da considerarsi come una imprescindibile bussola.