COMMISSIONI RIUNITE
AFFARI COSTITUZIONALI DELLA PRESIDENZA DEL CONSIGLIO E INTERNI (I)
DIFESA (IV)

RESOCONTO STENOGRAFICO

AUDIZIONE

1.

SEDUTA DI MARTEDÌ 7 MARZO 2017

PRESIDENZA DEL PRESIDENTE DELLA IV COMMISSIONE
DELLA CAMERA DEI DEPUTATI
FRANCESCO SAVERIO GAROFANI

INDICE

N. B. Sigle dei gruppi parlamentari: Partito Democratico: PD; MoVimento 5 Stelle: M5S; Forza Italia - Il Popolo della Libertà - Berlusconi Presidente: (FI-PdL); Articolo 1 - Movimento Democratico e Progressista: MDP; Area Popolare-NCD-Centristi per l'Europa: AP-NCD-CpE; Lega Nord e Autonomie - Lega dei Popoli - Noi con Salvini: (LNA); Scelta Civica-ALA per la Costituente Liberale e Popolare-MAIE: SC-ALA CLP-MAIE; Civici e Innovatori: (CI); Sinistra Italiana-Sinistra Ecologia Libertà: SI-SEL; Democrazia Solidale-Centro Democratico: (DeS-CD); Fratelli d'Italia-Alleanza Nazionale: (FdI-AN); Misto: Misto; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-Partito Socialista Italiano (PSI) - Liberali per l'Italia (PLI): Misto-PSI-PLI; Misto-Alternativa Libera-Possibile: Misto-AL-P; Misto-Conservatori e Riformisti: Misto-CR; Misto-USEI-IDEA (Unione Sudamericana Emigrati Italiani): Misto-USEI-IDEA; Misto-FARE ! - Pri: Misto-FARE ! - Pri; Misto-UDC: Misto-UDC.

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE
DELLA IV COMMISSIONE
DELLA CAMERA DEI DEPUTATI
FRANCESCO SAVERIO GAROFANI

La seduta comincia alle 13.20.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso l'attivazione di impianti audiovisivi a circuito chiuso, la trasmissione televisiva sul canale satellitare e la trasmissione diretta sulla *web-tv* della Camera dei deputati.

Audizione del Presidente dell'autorità Garante per la protezione dei dati personali, Antonello Soro, sulle problematiche legate alla difesa e alla sicurezza nello spazio cibernetico.

PRESIDENTE. L'ordine del giorno delle Commissioni riunite Affari costituzionali e Difesa reca l'audizione, ai sensi dell'articolo 143, comma 2, del regolamento, del Presidente dell'autorità Garante per la protezione dei dati personali, Antonello Soro.

L'audizione del Presidente Soro inaugura un breve ciclo di attività conoscitiva, convenuto dall'Ufficio di Presidenza congiunto delle due Commissioni, al fine di approfondire la conoscenza – per i rispettivi profili di competenza – delle problematiche legate alla difesa e alla sicurezza nello spazio cibernetico.

Ricordo che, come di consueto, dopo l'intervento del Presidente Soro potranno intervenire, per porre domande o formulare osservazioni, i colleghi che ne faranno richiesta, ai quali poi il Presidente Soro potrà rispondere.

Il Presidente Soro è accompagnato dal dottor Baldo Meo, Capo Ufficio stampa e Dirigente del servizio relazioni esterne e media del Garante, e dalla dottoressa Federica Resta.

Do subito la parola al Presidente Soro per lo svolgimento della sua relazione.

ANTONELLO SORO, *Presidente dell'autorità Garante per la protezione dei dati personali*. Grazie, presidente. Ringrazio le Commissioni che hanno voluto affrontare questo tema, tradizionalmente declinato in chiave esclusivamente pubblicistica, in una prospettiva che giustamente include anche il profilo dei diritti della persona e – in particolare – del diritto alla protezione dei dati, tutt'altro che antagonista rispetto alla sicurezza collettiva nella dimensione cibernetica, rappresentandone una delle principali componenti.

È utile ricordare che la funzione originaria della protezione dei dati nell'ordinamento europeo è stata considerata un bene giuridico che ciascuno Stato membro avrebbe dovuto tutelare al fine di potere entrare nell'area Schengen, in quanto presupposto per la sicurezza dell'area stessa.

Gli sviluppi più recenti dimostrano quanto tale concezione originaria del rapporto sinergico tra protezione dei dati e sicurezza fosse lungimirante. In un'economia e in una società fondate sui dati, proteggere questi significa proteggere, a un tempo, i singoli e la collettività. In una prospettiva di sicurezza e difesa è l'ambiente digitale che offre la principale superficie di attacco, contenitore di tutte le informazioni che riguardano le infrastrutture strategiche, dalla rete elettrica agli ospedali e agli aeroporti, ma soprattutto le nostre persone.

In questa nuova dimensione della vita, così come si è andata configurando, le per-

sone sono più vulnerabili, per cui la protezione dei dati personali è essa stessa essenziale presupposto non solo della *cybersecurity*, ma più in generale della sicurezza pubblica. Tale presupposto è tanto più necessario, se consideriamo che l'impostazione iniziale di internet ha privilegiato la funzionalità rispetto alla sicurezza.

Le recenti inchieste in tema di spionaggio cibernetico ai danni di singoli rappresentanti di imprese o istituzioni e le stesse controverse interferenze straniere nel procedimento elettorale statunitense confermano come quelli telematici siano i canali di ingresso elettivi per l'attacco dei bersagli da parte degli *hacker*, perché tali canali sono incomparabilmente più fragili di quelli propri della dimensione materiale e, nello stesso tempo, assai più importanti per accedere al controllo dei centri strategici del soggetto da colpire.

In questi anni, il *cybercrime* ha superato il mercato del narcotraffico. L'Istituto interregionale delle Nazioni Unite per la ricerca sul crimine e la giustizia ha stimato in oltre 500 miliardi di dollari l'entità annua dei danni al *business* mondiale.

Secondo le stime dell'Associazione Clusit, il 72 per cento degli attacchi verificatesi nell'ultimo anno a livello globale sarebbe stato effettuato per fini estorsivi o di sfruttamento dei dati personali. Le infrastrutture critiche sono state oggetto del 15 per cento in più di attacchi rispetto allo scorso anno e sarebbero cresciuti del 117 per cento gli attacchi riconducibili ad attività di *cyberwarfare*, che utilizzano i canali telematici per esercitare pressioni su scelte geopoliticamente rilevanti. Il recente rapporto della Banca d'Italia conferma sostanzialmente queste cifre.

Sarebbero cresciuti addirittura oltre il 1.000 per cento gli attacchi compiuti mediante *phishing* e tecniche di ingegneria sociale, che, come rileva anche la relazione del Dipartimento delle informazioni per la sicurezza (DIS), sfruttano soprattutto l'inesperienza degli utenti, a dimostrazione di come il fattore umano influenzi tuttora in maniera preponderante la sicurezza informatica.

Le diverse ricerche svolte in questo campo concordano nel sostenere che molte delle amministrazioni centrali e, ancora di più, quelle periferiche dello Stato siano caratterizzate da una vulnerabilità intrinseca.

Questo non è un dato riferito solo al nostro Paese, perché ricerche di carattere più generale hanno accertato che in un'elevatissima quantità di pubblici funzionari la *password* più utilizzata, forse fino all'anno scorso, era appunto la parola « *password* ».

Questo dimostra come la resilienza informatica debba oggi costituire il primo obiettivo su cui soggetti pubblici e privati sono tenuti a investire con risorse umane e finanziarie, attraendo il rischio informatico e cibernetico all'interno del rischio aziendale, con un profilo di gestione di tali criticità mutuato da quello che il Regolamento generale sulla protezione dei dati dell'Unione europea impone ai titolari.

Ciò si spiega considerando che la rete è il centro nevralgico dell'economia digitale, nella quale le informazioni sono il bene più prezioso e, come tali, oggetto di conflitti perché utilizzate, oltre che per fini di spionaggio, per scopi ritorsivi ed estorsivi.

Le relazioni ostili tra gli Stati e dentro gli Stati si svolgono prevalentemente nella dimensione digitale. Sin dall'attacco informatico all'Estonia del 2007, si è discusso se appunto in questi casi possa invocarsi un intervento della NATO, estendendo così alla realtà digitale gli strumenti pensati per la difesa dell'equilibrio internazionale da aggressioni di tipo tradizionale.

Con l'*affaire* del virus Stuxnet, una delle più potenti armi cibernetiche mai sviluppate, nel 2010, è stato dimostrato come un attacco informatico possa determinare, in via neppure indiretta, danni fisici ben maggiori di quelli di un attacco cinetico. La porta di ingresso e, a un tempo, il bersaglio di questi attacchi sono i dati non sufficientemente protetti, non solo per la coincidenza in alcune figure bersaglio del ruolo di privato e pubblico, ma più in generale perché le minacce cibernetiche si snodano attraverso il flusso dei dati, la cui protezione è elemento fondativo della *cybersecurity*.

Non è un caso che la recente Direttiva NIS sulla sicurezza delle informazioni e delle reti mutui proprio dalla disciplina di protezione dei dati alcuni istituti giuridici fondamentali, quali in particolare la comunicazione all'autorità competente – in caso di incidenti che abbiano determinato violazione di dati e sistemi, la cosiddetta « *data security breach* » – e le misure di sicurezza da adottarsi obbligatoriamente in chiave preventiva. È poi significativo che la sicurezza cibernetica sia stata definita bene comune e non rivale, la cui tutela avvantaggia tutti, perché attiene a una realtà, quella digitale, fondata sull'interdipendenza, oltre che sulla condivisione.

È rilevante che la principale distinzione tra sicurezza informatica e sicurezza cibernetica attenga proprio alla dimensione relazionale di quest'ultima e al valore che assegna alla protezione delle infrastrutture e dei domini digitali, considerati non atomisticamente, ma nella loro interrelazione.

Su questo orizzonte si proietta la nostra idea di protezione dei dati, come strettamente correlata alla protezione dei sistemi e delle infrastrutture, di cui abbiamo avuto modo di segnalare le vulnerabilità anche al Governo in varie occasioni.

Significativa in questo senso, anche perché emblematica, al di là del significato specifico di quella esperienza, è in particolare l'attività che abbiamo svolto rispetto ai principali nodi di interscambio internet, i cosiddetti « IXP », gestiti da consorzi privati, verificando evidenti criticità nelle misure di sicurezza. Tali soggetti mettono a disposizione degli *internet service provider* un'infrastruttura di rete comune, cui gli operatori possono collegarsi per scambiare in modo paritario il traffico telematico.

Dalla sicurezza di questa infrastruttura comune e dalla neutralizzazione del rischio che i gestori degli IXP accedano ai contenuti di traffico smistato dipendono non solo la riservatezza delle nostre comunicazioni, l'efficacia delle indagini e l'incolumità dei singoli, ma la stessa sicurezza cibernetica, quindi una delle principali componenti della sicurezza nazionale.

Non a caso, in occasione delle indagini a seguito del Datagate, è emerso che dati particolarmente rilevanti per quantità e qualità sarebbero stati acquisiti dalle agenzie di sicurezza degli Stati Uniti, appunto accedendo ai centri di interconnessione telematica.

È evidente, dunque, il rischio correlato alla permeabilità di tali infrastrutture, imputabile a una loro gestione inadeguata sotto il profilo delle *policy* di sicurezza, così come abbiamo riscontrato in alcuni IXP caratterizzati da una notevole vulnerabilità.

Per non rendere la fase dell'instradamento verso i *provider* del traffico dei dati una zona franca e non governata da regole, abbiamo in quell'occasione indicato ai gestori dei nodi di interscambio le cautele minime per elevarne lo standard di sicurezza. Successivamente, il Governo ha proceduto, con alcune misure, a mettere in sicurezza – o almeno, allo stato attuale, questo ci risulta – i nodi particolarmente rilevanti, perché questa sicurezza deve essere garantita anche nella fase di collegamento tra i sistemi e le reti, dunque nella fase di trasmissione del flusso telematico.

La sicurezza dei dati deve essere sempre di più un fattore abilitante per la stessa efficienza delle infrastrutture oltre che un obiettivo da perseguire fin dalla progettazione dei canali di comunicazione – in modo da rendere la tecnologia parte della soluzione, prima che del problema – e da responsabilizzare i privati che di tali infrastrutture abbiano la disponibilità. È questa anche l'impostazione posta alla base della *privacy by design*, richiesta dal nuovo Regolamento generale sulla protezione dei dati.

Lo spazio cibernetico, pur essendo un bene d'interesse comune, non è dal punto di vista domenicale un bene comune, appartenendo a una serie di soggetti (imprese o Stati) che ne controllano a vario titolo segmenti, tecnologie e nodi, mediante i quali passano le comunicazioni. La dipendenza da chi ha la titolarità di tali infrastrutture rende vulnerabili e dipendenti dalla loro azione, tanto che i *big tech*, come Microsoft e Google, starebbero cercando di rendersi indipendenti, con propri nodi e cavi, temendo non solo la concorrenza, ma soprat-

tutto limitazioni e controlli ingiustificati da parte di terzi.

La questione degli IXP è emblematica di alcuni degli aspetti essenziali della *cybersecurity*. In primo luogo, di fronte a minacce che vanno dalla guerra cibernetica all'antagonismo politico-digitale, il salto di qualità che si impone nella nostra strategia difensiva sta nell'investire non soltanto sulla protezione del punto terminale, che è dato irrinunciabile, ma anche nelle infrastrutture e nell'ecosistema digitale nel suo complesso, altrimenti avremmo monadi perfettamente protette, immerse in un reticolo di vulnerabilità.

La stretta dipendenza della sicurezza della rete da chi ne gestisce vari snodi e canali pone il tema della sovranità digitale, anche recentemente invocata a livello europeo. Questa, tuttavia, è una sovranità da non declinarsi in chiave nazionalistica o autarchica (per riportare all'interno dei confini territoriali il baricentro digitale degli Stati), quanto piuttosto nel segno dell'assunzione di responsabilità pubbliche rispetto alla *governance* telematica.

Per altro verso, è ineludibile l'esigenza di una responsabilizzazione adeguata dei privati, a vario titolo coinvolti nella complessa catena della sicurezza dei sistemi e delle reti, di cui gestiscono snodi importanti e dalla cui resilienza informatica dipende la protezione dei singoli e della collettività. Il ruolo dei privati è cruciale anche rispetto alla sempre più frequente esternalizzazione di segmenti importanti dell'attività investigativa. Si pensi alle intercettazioni e in particolare a quelle mediante captatori, forniti e in parte gestiti da privati, che ne rendono alquanto più permeabile, complessa e vulnerabile la filiera, come dimostra il caso di Hacking Team o anche il caso Area. La vulnerabilità dei sistemi utilizzati da tali privati espone a un rischio insostenibile i dati investigativi e, a volte, persino la sicurezza nazionale.

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

Si tratta di quanto persegue in particolare il nostro provvedimento del 2013 sulle misure di sicurezza dei dati trattati nell'ambito delle attività di intercettazione, che, pure con qualche vischiosità e ritardo da parte del sistema delle procure, sta per essere attuato quasi ovunque, uniformando gli standard di sicurezza. Quello della parcellizzazione dei centri di responsabilità è, del resto, un rischio cui ovviare necessariamente con la centralizzazione di competenze all'interno di una strategia unitaria, nazionale ed europea, come prevede la stessa Direttiva NIS.

In tal senso, resta significativa la necessità di attrarre la disciplina del coordinamento informativo e delle relative piattaforme informatiche nella competenza statale esclusiva, così da superare quella frammentazione che ha caratterizzato sinora il processo di informatizzazione del settore pubblico in Italia, il cui livello di sicurezza, ma anche di innovazione, è, come è noto, alquanto disomogeneo.

Altrettanto ineludibile è un'organica razionalizzazione del patrimonio informativo, anzitutto pubblico, essendo la riduzione della superficie d'attacco e del suo intrinseco rischio sociale la migliore difesa contro chi intende sfruttare le vulnerabilità inevitabilmente proprie di masse di dati difficilmente gestibili e, in alcune circostanze, poco utili perché scarsamente selettive.

Ciò vale tanto per i *big data*, di cui sempre più si alimenta la pubblica amministrazione, quanto per i *signal intelligence* e in generale per l'attività di indagine di tipo strategico, non immune dalla tentazione di allontanarsi da quel principio di proporzionalità tra *privacy* e sicurezza ed esigenze investigative, ribadito più volte dalla Corte di giustizia e di recente confermato con una sentenza, nota come Tele2, dello scorso dicembre, così da rendere uno strumento investigativo, come la *data retention*, ontologicamente massivo, invece che una misura selettiva da applicare a obiettivi mirati e in base a presupposti stringenti. Del resto, è alla garanzia del rispetto del

principio di proporzionalità e di un elevato livello di tutela dei dati personali, acquisiti anche nell'attività di *intelligence*, che mira il protocollo d'intenti siglato dal Garante con il DIS nel 2013, anche in ragione dei nuovi poteri attribuiti agli organismi in questa materia dalla legge n. 133 del 2012 e dalla Direttiva Monti.

L'elemento innovativo del protocollo consiste nella sistematicità e nello stesso ambito oggettivo degli accertamenti, inerenti non a uno specifico trattamento, ma alle modalità organizzative e procedurali utilizzate per la legittimità delle operazioni complessivamente intese.

Tale forma di esercizio dei poteri di garanzia dell'autorità è maggiormente compatibile con le peculiarità assunte dall'attività di *intelligence,* incentrandosi più specificamente sulla sicurezza dei dati e dei sistemi con i quali i vari trattamenti sono svolti, che non soltanto sulla legittimità del singolo puntuale trattamento. Del resto, quello della funzione di garanzia dell'autorità di protezione dei dati in un contesto di progressivo ampliamento dei poteri informativi dell'*intelligence* è un tema condiviso in ambito europeo, che ci è valso un apprezzamento particolare per il lavoro svolto con il protocollo in questi anni.

Su questo terreno, il nostro codice, tra i pochi in Europa ad attribuire all'autorità di protezione dei dati una specifica competenza sull'*intelligence*, ha rivelato tutta la sua lungimiranza e, in questa parte, resterà immutato anche nella vigenza del nuovo quadro giuridico europeo. Grazie.

PRESIDENTE. Grazie presidente Soro. Do ora la parola ai deputati che intendano porre quesiti o formulare considerazioni.

MASSIMO ARTINI. Ringrazio il presidente Soro per la trattazione sul tema, che effettivamente mi ha colpito in molte punti, soprattutto, andando nel dettaglio, per quanto riguarda la parte sulla sovranità, la parte normativa e quella sulla *privacy*, che poi fondamentalmente è di sua stretta competenza.

Le faccio alcune domande in merito all'attuale struttura di *governance* del sistema *cyber* e, anche se non ancora pubblicata, alla modifica fatta da uno degli ultimi Consigli dei ministri, in cui al DIS è stata attribuita ancora più forza, soprattutto per dare seguito alla Direttiva europea NIS.

In primo luogo, ai sensi dell'articolo 157 della legge n. 196 del 2003, che organizza e norma tutta la parte di gestione sulla *privacy*, un cittadino può richiedere, per il tramite dell'Autorità, l'accesso alle banche dati per conoscere eventualmente dove sono le informazioni. Il problema che si pone con la struttura – che per me ha dei forti problemi di *governance*, dovendo dare ai servizi segreti o comunque al DIS questo ruolo – è che poiché voi avete il titolo o comunque l'autorità per poter accedere a dati che possano essere considerati classificati, esiste un problema di tutela della *privacy* per il cittadino se si continua a mantenere quel sistema in capo ai servizi.

La seconda parte della domanda si riconduce a quello che lei ha comunque segnalato nella sua relazione, ovvero se ritiene che una ristrutturazione normativa e non regolamentare sia necessaria per dare seguito a questo tipo di passaggi e attuare realmente la Direttiva NIS (*Network and Information Security*). Questa Direttiva europea, che poi sia o meno recepita nelle varie leggi di delegazioni o leggi europee da parte del Parlamento, indica alcuni passaggi particolari in dettaglio, creando un'agenzia autonoma che possa gestire questo passaggio e che non ricada espressamente sotto la gestione dei servizi. Ebbene, vorrei sapere se secondo lei, per dare seguito a questo, sarebbe più opportuno procedere attraverso una apposita attività normativa.

Riguardo alla sovranità, sono d'accordo con lei sul fatto che non ci debba essere il ripristino di un nazionalismo cibernetico, difficilmente anche concepibile da un punto di vista tecnologico, ma il punto è – e torno alla parte fondamentale del suo mandato – la trattazione dei dati, che dovrebbero avere una sovranità, cioè avere una maggiore protezione da parte dell'organo pubblico. Il ragionamento che faccio è: in che termini si può esprimere la sovranità, se – lei ha

citato ad esempio Google e Microsoft, che si stanno attrezzando per avere proprie dorsali – come Paese non abbiamo o comunque non ci dotiamo di capacità industriali e logiche, come *software* e altro, che ci permettano di essere sovrani. Mi riferisco alla parte logica o *software* antivirus o sistemi di protezione nazionali sviluppati e non verticalizzati dallo Stato o comunque su commissione di aziende che possano essere iscritte a un elenco di aziende confidenti per lo Stato.

Lo stesso vale per la parte industriale, cioè per la parte di quel passaggio iniziale da lei fatto riguardo al trattamento del flusso dei dati, perché su alcuni nodi avere dei sistemi industriali che ci permettano di avere il pieno controllo della parte *hardware* sarebbe, a mio modo di vedere, uno spunto fondamentale. Quindi, le chiedo un parere anche su quest'aspetto.

PAOLA BOLDRINI. Grazie, presidente Soro, per la relazione molto interessante, soprattutto perché, oggi, stiamo guardando l'aspetto della sicurezza informatica. Peraltro, ho avuto il piacere di ascoltare il Presidente Soro anche nell'audizione della Commissione affari sociali, perché altra *privacy* molto importante è quella dei dati sanitari. Dico questo *incipit* perché vorrei sottolineare alcune cose.

La sua è stata un'interessantissima relazione, però sono evidenti alcuni aspetti. Vorrei innanzitutto capire come si può andare incontro a questo nuovo sistema informatico, che evolve sempre di più, per cui – a mio parere – anche lo Stato e le istituzioni pubbliche si dovrebbero evolvere in maniera così importante.

Tuttavia, sappiamo che soprattutto la tecnologia più innovativa è in mano ai privati. I *server* più importanti e i *big data* sono di Google e di Microsoft o, comunque, dei privati e non di istituzioni pubbliche. Quindi, noi scontiamo un po' un *deficit* innovativo. Infatti, sappiamo – e lei ne ha parlato – del problema della informatizzazione delle nostre pubbliche amministrazioni. Inoltre, forse, scontiamo anche un'informazione più deficitaria nella pubblica amministrazione. Lo dico perché anch'io sono un pubblico dipendente. Dovremmo forse avere ben presente cos'è la sicurezza dei dati quando questi vengono lavorati, e anche che, come mi diceva un mio collega tecnico informatico, qualsiasi cosa passi attraverso un sistema informatico lascia una traccia. È come se noi segnassimo tutto su una tavola di pongo o di plastilina, per cui tutto è tracciabile, e questo rappresenta un grosso problema.

In più, le pubbliche amministrazioni devono essere sempre più trasparenti, e su quest'aspetto si sta spingendo moltissimo, perché le amministrazioni adesso devono addirittura rendere molti documenti in formato libero, e sono così utilizzabili. A riguardo sono un po' perplessa perché è giusto che ci sia trasparenza e che tutti i cittadini conoscano tutto di tutti, però credo anche che bisogna bene rapportare la proporzionalità di cui prima si parlava fra *privacy* e sicurezza.

Dovremmo capire che bisogna innanzitutto investire di più per avere una dotazione autonoma come Stato e come pubbliche amministrazioni e per non avere sempre la necessità di ricadere nel privato. Inoltre, occorre fare molto più monitoraggio. Certo, ci sono già dei regolamenti e già tutto è predisposto, però sarebbe utile anche avere dei dati per capire se funziona questo tipo di interventi.

Quanto al tema della pubblica amministrazione – poiché non è passato tanto tempo dai primi *computer*, ma saranno passati trenta o quarant'anni e, quindi, nell'amministrazione pubblica abbiamo una vecchia generazione che ancora non si rende conto di queste cose – bisogna puntare molto di più sulla formazione rispetto all'informazione tecnologica e alle eventuali problematiche nelle quali si potrebbe cadere se non si hanno dovute informazioni. Grazie.

PRESIDENTE. Do la parola al Presidente Soro per la replica.

ANTONELLO SORO, *Presidente dell'autorità Garante per la protezione dei dati personali*. L'onorevole Artini pone alcuni problemi, sui quali naturalmente abbiamo tutti bisogno di riflettere. Il nuovo decreto

del Presidente del Consiglio dei ministri, che verrà all'esame delle Commissioni e su cui credo dovremmo esprimere il parere anche noi, quindi lo vedremo nel concreto, dà l'idea di anticipare in qualche modo la direttiva NIS, facendo convergere l'architettura *cyber* nei confronti di un soggetto, che nel nostro ordinamento è appunto protetto da particolari tutele parlamentari e giurisdizionali dall'autorità, quindi in un sistema democratico. Credo che questo sia un elemento positivo che concorra a creare insieme efficienza e controllabilità del sistema.

Valuteremo poi il contenuto specifico e più puntuale, ma l'idea in sé, così com'è stata illustrata dal direttore e così come abbiamo avuto modo di leggere, ci sembra positiva.

I temi in generale che lei, onorevole Artini, poneva richiederanno certamente, nell'evoluzione di questo sistema, anche interventi normativi, ma già la ratifica della Direttiva è un momento in cui il legislatore ha modo di esprimere e di aggiornare una serie di elementi, che la veloce innovazione dei sistemi tecnologici, ma anche, in questo caso, delle relazioni che sono intervenute in Europa, renderà necessario.

Con specifico riferimento ai dati classificati e al ruolo del Garante, vorrei dire che noi abbiamo, per effetto del codice in materia di protezione dati, la possibilità di accedere anche a dati classificati, con una procedura tutta particolare, nel senso che il componente dell'organo del Garante può accedere a questi dati e non può riferirne per iscritto, se non a voce al collegio del Garante, quindi c'è una serie di misure di protezione.

Devo dire che il vero tema, però, non è il controllo del singolo atto classificato, quanto piuttosto – questo è il salto in avanti fatto col protocollo – la capacità di controllare la correttezza delle procedure, attraverso le quali opera il sistema dell'*intelligence*, che deve rispettare una serie di regole che discendono dall'ordinamento europeo e italiano in materia di protezione dati.

L'altro tema, che riguarda più in generale la protezione dei dati, è la innovazione tecnologica, ossia le due facce sulle quali si gioca la partita della rincorsa che il sistema giuridico e che il diritto in tutte le parti fa nei confronti dell'innovazione tecnologica. Si tratta di una bella sfida che non riguarda solo il nostro Paese, anche se questa non è una consolazione, perché riguarda in generale tutti i Paesi del mondo, anche quelli che sono andati molto avanti negli anni passati.

Il meccanismo in qualche modo non previsto di un singolo gruppo d'impresa che tende a diventare monopolista oppure oligopolista nel mondo produce non solo una particolare ricchezza di risorse economiche, che consentono poi di investire ulteriormente nella ricerca, ma hanno anche una tale quantità di elementi di nuova conoscenza. Tutti gli studi sull'intelligenza artificiale nascono presso pochi soggetti perché questi hanno gli elementi di base, i grandi dati, i grandi volumi d'informazione e le grandi attrezzature di calcolo, che consentono di trarre nuova conoscenza con carattere predittivo e di anticipare in qualche modo quello che nel mondo si verifica, creando un momento in cui la geografia del rapporto di potere fra gli Stati, i Governi e i detentori di questo potere si è profondamente modificata.

Questo è un tema che sfida la democrazia in tutto il mondo. Il nostro Paese fa parte di un sistema, quello europeo, che ha cercato in questi anni di attrezzare il proprio ordinamento per affrontare questa realtà, con risorse e investimenti, come l'ipotesi del *cloud* europeo e altre possibilità di investimento unitario, perché le tecnologie in favore della protezione dei dati crescano molto in Europa per metterci al passo con la sfida che arriva da quella innovazione. Tali risorse e strumenti si devono accompagnare con la necessità di promuovere e di stimolare un riconoscimento universale del diritto alla protezione dei dati, nei termini in cui si è cercato nel passato di riconoscere il diritto alla protezione dell'ambiente, come un interesse universale e come una sfida per il mondo non per un singolo Paese.

È dentro questo orizzonte che si può collocare la sfida della protezione dei dati

personali, non considerata come un retaggio di una vecchia esigenza individualistica anacronistica, ma come la vera sfida in cui l'umanità si confronta rispetto alla innovazione delle tecnologie e ai nuovi poteri che alterano pesantemente in alcuni momenti o rischiano di alterare il ruolo degli Stati e dei Governi nella democrazia del mondo. Questo è un grande tema rispetto al quale la parte che a noi compete è quella di sviluppare molto i principi che stanno dentro la protezione dei dati. Mi allaccio, così, a un tema posto dall'onorevole Boldrini.

Come si governa questa innovazione ? Intanto dovremmo partire dalle competenze che abbiamo. Lei faceva cenno alla trasparenza, che è solo l'ultimo tassello, non tanto del sistema delle leggi quanto dell'atteggiamento culturale, che, per una buona e santa ragione, quella della trasparenza, finisce col mettere nella rete e nella dimensione digitale un'infinità di dati inutili ai fini della trasparenza, rendendo in questo modo più vulnerabili le persone, cui quei dati corrispondono.

L'idea che i dati vengano ancora considerati come una cifra e non come persone che stanno dietro quei dati è la prima carenza della cultura arretrata in tema di protezione dei dati e di *privacy*, usata spesso come una ragione di freno rispetto alla crescita della democrazia e allo sviluppo dell'economia.

Si verifica esattamente il contrario, perché tutte le volte che noi veniamo meno al principio di proporzionalità, uno dei capisaldi dell'ordinamento europeo e della cultura giuridica europea, o quando veniamo meno al principio della minimizzazione dei dati che noi mettiamo in rete, noi stiamo facendo torto a noi stessi, alla nostra generazione e a quella che verrà dopo di noi, perché stiamo mettendo dentro una dimensione con presidi minori rispetto a quelli della dimensione materiale, che ha consolidato nei secoli culture, regole e diritto. Quindi, il tema vero è interpretare quei principi in ogni atto legislativo che noi facciamo, nei comportamenti e nella cultura.

Bisogna sapere che la dimensione digitale non è un pozzo vuoto, a perdere, ma è un posto dove tutto rimane, in una società nella quale già oggi tutto è sorvegliato dagli imprenditori privati, che, per ragioni di profilazione, raccolgono tutti i nostri dati, ed è sorvegliato dai Governi di tutto il mondo, che, per ragioni di sicurezza, raccolgono su tutto quello che è possibile e spesso lo fanno inutilmente.

L'esperienza degli Stati Uniti ha dimostrato quanto fosse inutile, oltre che poco attenta ai diritti, la raccolta massiva di dati di tutti i cittadini non americani che comunicavano con cittadini americani. Questi dati venivano interamente raccolti e ribaltati in grandi calcolatori, che avrebbero dovuto poi trarne fuori ragioni per potenziare le difese degli Stati Uniti, ma questo non è servito a nulla.

Può darsi che la sicurezza degli Stati Uniti cambierà, ma non lo so e spero di no. Comunque, il fatto che il Governo degli Stati Uniti, soltanto qualche mese fa, ha accettato di sottoscrivere con l'Europa il *Privacy shield*, cioè un nuovo accordo in materia di protezione dei dati dei cittadini europei, rispettando quelle regole e quei princìpi, significa non solo l'accettazione di un'esigenza commerciale e materiale, ma anche il riconoscimento dell'inutilità di una raccolta massiva, che nessuno poi è in grado di analizzare nel dettaglio, se non c'è dietro il ruolo del fattore umano dell'investigatore, che è insostituibile e che deve avvalersi della capacità selettiva di utilizzo delle tecnologie, ma non può delegare alle tecnologie problemi e questioni che riguardano prima di tutto la responsabilità delle persone.

Questo mi pare che naturalmente debba essere tradotto, come lei suggeriva, anche nella formazione della pubblica amministrazione, anche se si tratta di compito arduo, però ineludibile.

PRESIDENTE. Ringrazio il Presidente Soro per le cose che ha detto e per la sua disponibilità a partecipare ai nostri lavori.

Dichiaro conclusa l'audizione.

La seduta termina alle 14.

Licenziato per la stampa
il 14 dicembre 2017

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA

17STC0027210