**Il CESE lancia delle proposte per fare della cibersicurezza una realtà**

**L'UE dovrebbe, tra le altre cose, rafforzare il mandato dell'ENISA in quanto agenzia dell'UE per la cibersicurezza, creare un quadro di certificazione a livello europeo e concentrarsi sull'istruzione e la protezione degli utenti di Internet.**

In un [parere](http://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/cybersecurity-act) adottato alla sua sessione plenaria del 14 febbraio 2018, di cui sono relatori **Alberto Mazzola** e **Antonio Longo** della sezione specializzata Trasporti, energia, infrastrutture, società dell'informazione (TEN), il CESE sostiene in linea generale il regolamento sulla cibersicurezza, che la Commissione ha presentato al Consiglio nel settembre 2017 nel quadro del [pacchetto sulla cibersicurezza](https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en).

Il tema della cibersicurezza è di attualità in tutto il mondo: si tratta di una sfida globale dato che gli attacchi possono verificarsi ovunque. Da una specifica indagine di Eurobarometro in merito all'atteggiamento degli europei nei confronti della cibersicurezza risulta che il 73% degli utenti di Internet teme che i siti Internet potrebbero non custodire in modo sicuro i dati personali forniti online, e il 65% teme che le autorità pubbliche potrebbero non custodirli in modo sicuro. La maggior parte degli interpellati teme di essere vittima di varie forme di criminalità informatica, specialmente software malevoli (*malware*) introdotti nei loro dispositivi (69%), furto d'identità (69%) e frodi attraverso carte bancarie e operazioni bancarie online (66%).

Al fine di rafforzare il quadro europeo della cibersicurezza, il CESE propone una serie di misure pratiche.

* **Rafforzare l'ENISA in quanto agenzia dell'UE per la cibersicurezza**

L'**Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA)**, che ha sede in Grecia, è un centro europeo specializzato nella cibersicurezza. Il CESE condivide il giudizio della Commissione secondo cui il mandato dell'ENISA dovrebbe essere reso permanente, ma ritiene anche che dovrebbe essere dotata di risorse finanziarie maggiori e che la sua azione dovrebbe concentrarsi sul sostegno della pubblica amministrazione online (*e-government*), specie per quanto riguarda l'identità digitale per le persone e le organizzazioni nell'UE e nel mondo, la prevenzione e la repressione del furto d'identità e della frode online e la lotta contro il furto di proprietà intellettuale.

È inoltre essenziale intensificare la cooperazione tra i soggetti interessati, e a tal fine potrebbe essere utile rafforzare la cooperazione con gli Stati membri e istituire una rete formale di agenzie nazionali per la cibersicurezza. L'ENISA avrebbe quindi il potere di sottoporre ad audit gli organismi nazionali, instaurando in tal modo un clima di fiducia tra tutte le agenzie. "È importante che tutti gli Stati membri istituiscano un organismo nazionale per la cibersicurezza", ha osservato **Mazzola**. "Oggi, più della metà degli Stati membri non dispone di un organismo omologo dell'ENISA. La Commissione europea dovrebbe fare in modo che vengano raccolte e condivise le buone pratiche nazionali e le misure efficaci".

Il CESE raccomanda di coinvolgere e far cooperare tutte le agenzie settoriali dell'UE, e in particolare l'Autorità bancaria europea (EBA), l'Agenzia europea per la sicurezza aerea (EASA), l'Agenzia europea per i medicinali (EMA) e l'Agenzia dell'Unione europea per le ferrovie (ERA), al fine di compensare la mancanza di risorse dell'ENISA e di mettere a frutto le loro competenze specifiche.

* **Maggiori investimenti strategici**

Il CESE sottolinea che l'UE dovrebbe aumentare, attraverso una forte cooperazione tra settore pubblico e settore privato, gli investimenti diretti verso obiettivi strategici nel campo della cibersicurezza. Le risorse potrebbero derivare da diversi fondi europei e nazionali, da investimenti del settore privato e da un **Fondo UE** **per la cibersicurezza**, istituito appositamente.

Più specificamente, il Comitato propone di trasformare l'attuale partenariato pubblico-privato contrattuale (cPPP) in un'impresa comune tripartita (Commissione europea, Stati membri e imprese), cosa che non solo aumenterebbe le risorse, ma contribuirebbe anche alla fiducia tra le parti interessate. L'UE dovrebbe inoltre considerare l'apertura di una nuova finestra nell'attuale e nel futuro meccanismo per collegare l'Europa, come pure nel prossimo FEIS 3.0.

* **Una rete di competenza dell'UE in materia di cibersicurezza**

Per essere realmente competitiva sulla scena mondiale e creare una solida base tecnologica, l'UE deve acquisire la "sovranità digitale". A questo proposito, il CESE concorda con la Commissione nel ritenere indispensabile creare una **rete di competenze dell'UE in materia di cibersicurezza**, sulla base di un quadro coerente a lungo termine, che comprenda tutti gli elementi della catena del valore della cibersicurezza.

Tale rete fungerebbe da fornitore di competenze tecniche e di formazione in materia di igiene informatica e, contribuendo a ridurre la dipendenza dalle competenze di paesi terzi per le capacità tecnologiche essenziali, promuoverebbe una base industriale europea competitiva.

Un **Centro di ricerca e competenza sulla cibersicurezza** a livello europeo sosterrebbe la rete facendo da collegamento tra gli attuali centri di competenza nazionali di tutta l'UE. Esso coordinerebbe i progetti di ricerca, creando un vero e proprio ecosistema europeo della cibersicurezza, in cui può realizzarsi l'innovazione.

* **Una certificazione europea della cibersicurezza**

Il Comitato ritiene che si dovrebbe istituire un **quadro europeo di certificazione della cibersicurezza**, con requisiti differenti in funzione dei diversi settori. I regimi di certificazione contribuirebbero ad aumentare la sicurezza in base alle attuali esigenze e alla conoscenza delle minacce, e dovrebbero fondarsi su norme europee, definite congiuntamente, in materia di cibersicurezza e TIC a livello internazionale.

Un quadro di certificazione potrebbe anche fornire una base comune per affrontare il problema della frammentazione in materia di cibersicurezza. Un'interpretazione omogenea delle norme, compreso il riconoscimento reciproco tra gli Stati membri in un quadro unificato, faciliterebbe in particolare la protezione del mercato unico digitale.

* **Un sistema di etichettatura riconosciuto a livello europeo**

Il processo di certificazione dovrebbe includere un adeguato **sistema di etichettatura**, sia per l'hardware che per il software, da applicare anche a prodotti importati da paesi terzi. I vantaggi del sistema di etichettatura sono molteplici: ridurre i costi per le imprese, eliminare le frammentazioni esistenti sul mercato a causa di diversi sistemi nazionali di certificazione e semplificare la comprensione, da parte dei consumatori, delle caratteristiche dell'oggetto acquistato.

Il CESE ritiene che sarebbe vantaggioso, per rafforzare la fiducia dei consumatori, creare un **logo ad hoc**, ad esempio un "lucchetto" collocato all'inizio della barra degli indirizzi di un sito web, che richiamerebbe immediatamente l'attenzione degli utilizzatori, informandoli circa l'affidabilità dei prodotti e dei siti web.

* **Il fattore umano: istruzione e protezione**

Gli utenti sono soggetti fondamentali dei processi digitali, perché traggono vantaggi dall'uso di Internet, ma allo stesso tempo possono anche essere vittime di gravi incidenti informatici. Il Comitato ritiene che la proposta della Commissione dovrebbe andare più in là e concentrarsi sul **miglioramento delle competenze informatiche** dei singoli cittadini e delle imprese.

Per accrescere l'igiene e la consapevolezza informatica, il CESE raccomanda tre linee di azione, basate sull'apprendimento permanente e su programmi di formazione, su campagne di sensibilizzazione, e sulla creazione di un programma di studi certificato dall'UE per gli istituti d'istruzione superiore e i professionisti.

"Le persone sono essenziali per trasformare la cibersicurezza in una realtà. Sono utenti e consumatori. Dobbiamo investire nell'istruzione e nella formazione, per creare una solida base di competenze informatiche, rafforzare la conoscenza di un comportamento informatico "sicuro" e promuovere nel contempo la fiducia degli utenti nei confronti di Internet. A tal fine, è essenziale che le autorità nazionali e regionali, le imprese e le PMI si uniscano in un approccio collettivo", ha sottolineato **Longo**.

* **L'Internet degli oggetti *(IoT)***

Il fattore umano svolge un ruolo centrale anche nei comuni dispositivi dell'Internet delle persone *(IoP)* che utilizziamo nella vita quotidiana, ad esempio le componenti digitali di automobili e case. Ci affidiamo a una crescente quantità di dispositivi connessi, che spesso non sono protetti come i dispositivi tradizionali, e offrono agli autori di reati informatici maggiori opportunità. Una certificazione dell'UE potrebbe quindi fornire un maggiore livello di sicurezza per il cosiddetto **Internet degli oggetti *(IoT)***.