Consiglio
dell'Unione europea

Bruxelles, 2 dicembre 2020
(OR. en)

13629/20

CYBER 263
TELECOM 248
COPEN 362
CODEC 1266
COPS 441
COSI 235
CSC 344
CSCI 86
IND 248
RECH 493
ESPACE 77

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
in data:	2 dicembre 2020
Destinatario:	Delegazioni
Oggetto:	Conclusioni del Consiglio sulla cibersicurezza dei dispositivi connessi - Conclusioni del Consiglio approvate mediante procedura scritta

Si allegano per le delegazioni le conclusioni del Consiglio sulla cibersicurezza dei dispositivi connessi, approvate dal Consiglio mediante procedura scritta il 2 dicembre 2020.

ALLEGATO

Conclusioni del Consiglio sulla cibersicurezza dei dispositivi connessi

Il Consiglio dell'Unione europea,

RAMMENTANDO

- le conclusioni del Consiglio sulla comunicazione congiunta al Parlamento europeo e al Consiglio "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE";
- le conclusioni del Consiglio sullo sviluppo di capacità e competenze in materia di cibersicurezza nell'UE;
- le conclusioni del Consiglio sull'importanza del 5G per l'economia europea e sulla necessità di attenuare i relativi rischi per la sicurezza;
- le conclusioni del Consiglio sul futuro di un'Europa altamente digitalizzata oltre il 2020: "Accrescere la competitività digitale ed economica e la coesione digitale in tutta l'Unione";
- le conclusioni del Consiglio dal titolo "Plasmare il futuro digitale dell'Europa";
- le conclusioni del Consiglio europeo concernenti la COVID-19, il mercato unico, la politica industriale, il digitale e le relazioni esterne;
- la comunicazione della Commissione europea dal titolo "Plasmare il futuro digitale dell'Europa",

1. SOTTOLINEA la necessità che l'Unione europea e i suoi Stati membri garantiscano la loro sovranità digitale e la loro autonomia strategica, preservando nel contempo un'economia aperta. Ciò include il rafforzamento della capacità di compiere scelte tecnologiche autonome e, in quanto uno dei principali pilastri, di infrastrutture, prodotti e servizi resilienti e sicuri per accrescere la fiducia nel mercato unico digitale e all'interno della società europea.
I valori fondamentali dell'Unione europea preservano in particolare la vita privata, la sicurezza, l'uguaglianza, la dignità umana, lo Stato di diritto e l'internet aperta come prerequisiti per realizzare una società, un'economia e un'industria antropocentriche e orientate al settore digitale;

2. RICONOSCE la crescente importanza dei dispositivi connessi e della loro sicurezza, compresi i macchinari, i sensori e le reti che costituiscono l'internet delle cose. I dispositivi connessi svolgeranno un ruolo chiave nell'ulteriore definizione del futuro digitale dell'Europa, dal punto di vista industriale e imprenditoriale, nonché nella vita quotidiana dei consumatori di una nuova generazione di tecnologie. Oltre alle reti 5G, l'intelligenza artificiale, la computazione quantistica, il calcolo ad alte prestazioni, il cloud computing, la tecnologia del registro distribuito segnatamente la blockchain e qualsiasi altra nuova applicazione e opportunità per una crescita economica sostenibile e un livello più elevato di digitalizzazione della nostra società possono essere realizzati solo mediante dispositivi connessi sicuri sotto il profilo informatico;

3. OSSERVA che l'utilizzo crescente di prodotti di largo consumo e dispositivi industriali connessi a internet comporterà anche nuovi rischi per la vita privata, la sicurezza delle informazioni e la cibersicurezza, tra cui un continuo aumento delle potenziali conseguenze sull'integrità e la disponibilità di prodotti e dati, con possibili ripercussioni dirette sulla sicurezza. È essenziale ridurre al minimo tali rischi al fine di proteggere i consumatori, rafforzare la ciberresilienza complessiva dell'Europa e accrescere la fiducia dei cittadini nelle soluzioni e nelle tecnologie digitali. Ciò favorirà anche la competitività e le capacità di innovazione dei fornitori europei di tali dispositivi. La cibersicurezza e la tutela della vita privata dovrebbero essere riconosciute come requisiti essenziali per l'innovazione dei prodotti e i processi di produzione e sviluppo, compresa la fase di progettazione ("sicurezza fin dalla progettazione"), e dovrebbero essere garantite lungo l'intero ciclo di vita del prodotto e lungo tutta la sua catena di approvvigionamento;

4. EVIDENZIA che, oltre a garantire un elevato livello di sicurezza dei dispositivi connessi, è altrettanto importante sensibilizzare i consumatori in merito ai potenziali rischi per la loro vita privata e la loro sicurezza. Ciò contribuirebbe a ridurre al minimo le minacce derivanti dall'utilizzo crescente dei dispositivi connessi, a rafforzare la fiducia nel mercato unico digitale e a sfruttare al massimo i vantaggi economici e sociali offerti dalle tecnologie dei dispositivi connessi;

5. SOTTOLINEA che gli investimenti pubblici nella ricerca e nell'innovazione, segnatamente attraverso Orizzonte Europa e Europa digitale, nonché gli investimenti privati potrebbero creare preziosi incentivi per aumentare la sicurezza e la protezione dei dispositivi connessi e, pertanto, anche la resilienza delle reti di comunicazione intelligenti. È inoltre opportuno accelerare gli investimenti nelle infrastrutture e tecnologie digitali necessarie per diffondere le più recenti tecnologie dei dispositivi connessi, al fine di conseguire una leadership industriale e digitale e garantire l'autonomia strategica, preservando nel contempo un'economia aperta;

6. RIMARCA la necessità di garantire un livello elevato di complementarità e comparabilità delle funzionalità di sicurezza dei sistemi e delle componenti TIC, che sono utilizzati in svariati settori del mercato unico digitale;

7. RICONOSCE gli attuali sviluppi a livello dell'Unione volti ad accrescere il livello di cibersicurezza dei dispositivi connessi, con particolare riguardo alle recenti iniziative della Commissione intese ad affrontare gli aspetti a breve termine della cibersicurezza nei pertinenti atti giuridici, ad esempio gli atti ai sensi del nuovo quadro legislativo, in particolare la direttiva 2014/53/UE (direttiva sulle apparecchiature radio). PONE L'ACCENTO sull'importanza di valutare la necessità, nel lungo termine, di un atto legislativo orizzontale, che specifichi anche le condizioni necessarie per l'immissione sul mercato, per affrontare tutti gli aspetti attinenti alla cibersicurezza dei dispositivi connessi, quali la disponibilità, l'integrità e la riservatezza. ACCOGLIE CON FAVORE, a tale proposito, una discussione intesa a esaminare l'ambito di applicazione di tale normativa e i suoi collegamenti con il quadro di certificazione della cibersicurezza quale definito nel regolamento sulla cibersicurezza, al fine di aumentare il livello di sicurezza all'interno del mercato unico digitale;

8. SOTTOLINEA che i requisiti di cibersicurezza dovrebbero essere definiti in linea con la pertinente legislazione dell'Unione, tra cui il regolamento sulla cibersicurezza, il nuovo quadro legislativo, il regolamento sulla normazione europea e un eventuale futuro atto legislativo orizzontale, al fine di evitare ambiguità e frammentazioni della legislazione;

9. RICONOSCE l'importante ruolo svolto da tutte le parti interessate, in particolare dai fabbricanti, al fine di aumentare il livello di cibersicurezza dei dispositivi connessi nel mercato unico digitale e INVOCA pertanto un coordinamento e una stretta cooperazione con tutte le parti interessate pubbliche e private pertinenti, anche in vista di un eventuale futuro atto legislativo orizzontale;

9 bis. SI COMPIACE dei lavori in corso condotti dall'ENISA per elaborare i primi sistemi di certificazione della cibersicurezza dell'UE, vale a dire la proposta di criteri comuni dell'Unione europea e la proposta di sistemi di servizi cloud. Tali sistemi costituiranno le basi pertinenti per la certificazione dei dispositivi connessi;

10. SOTTOLINEA che qualsiasi sistema di certificazione supplementare per i dispositivi connessi e i servizi correlati che sia previsto nel programma di lavoro progressivo dell'Unione e definito nell'ambito del regolamento sulla cibersicurezza dovrebbe specificare in che modo i requisiti di sicurezza applicabili al pertinente livello di affidabilità debbano essere soddisfatti sulla base di specifiche norme riconosciute a livello europeo e internazionale, indipendentemente dal settore in cui il prodotto sarà utilizzato, e quali specifiche di prova, certificati, ecc. debbano essere applicati;

11. RICONOSCE che la certificazione dei dispositivi connessi richiederebbe norme, standard o specifiche tecniche pertinenti per le valutazioni della cibersicurezza nell'ambito del regolamento sulla cibersicurezza. EVIDENZIA pertanto la necessità di stabilire norme, standard o specifiche tecniche in materia di cibersicurezza per i dispositivi connessi e RACCOMANDA di intensificare gli sforzi intrapresi in materia dalle organizzazioni europee di normazione. PRENDE ATTO nel contempo della norma ETSI EN 303 645 sulla cibersicurezza per i dispositivi dell'internet delle cose di largo consumo quale passo importante in questa direzione;

12. INVITA la Commissione a prendere in considerazione la possibilità di richiedere una proposta di sistemi di certificazione della cibersicurezza per i dispositivi connessi e i servizi correlati sulla base del programma di lavoro progressivo dell'Unione attualmente in fase di sviluppo, tenendo nella massima considerazione i sistemi europei orizzontali di certificazione della cibersicurezza attualmente in fase di sviluppo. Tale sistema su base volontaria consentirà ai fabbricanti di tali prodotti di promuovere prodotti con il livello di affidabilità valutato;

13. INVITA a una discussione su come integrare l'obiettivo della cibersicurezza in un futuro atto legislativo orizzontale che copra i rischi per la cibersicurezza relativi ai dispositivi connessi e, al tempo stesso, RILEVA la necessità di prendere in considerazione l'adeguamento, se del caso, dei requisiti essenziali delle rispettive direttive del nuovo quadro legislativo;

14. INCORAGGIA la Commissione a valutare anche, ove necessario, le normative settoriali complementari che dovrebbero definire il livello di cibersicurezza che il dispositivo connesso dovrebbe soddisfare per garantire l'introduzione di requisiti specifici di sicurezza e tutela della vita privata per i dispositivi che presentano rischi più elevati in termini di sicurezza;

15. SOTTOLINEA la necessità di migliorare la qualità della vita e il benessere dei cittadini europei e di promuovere la fiducia nel mercato unico digitale. La sicurezza e la tutela della vita privata nelle nostre società sono essenziali per preservare i valori fondamentali dell'Unione. INSISTE pertanto sull'esigenza di basarsi sul quadro fornito dal regolamento sulla cibersicurezza per armonizzare i requisiti di sicurezza, in funzione dei diversi livelli di affidabilità e in tutti i settori del nuovo quadro legislativo, al fine di evitare frammentazioni e controlli multipli di requisiti identici e offrire condizioni di parità in tutta l'Unione europea per la concorrenza e l'innovazione;

16. INVITA la Commissione, l'Agenzia dell'UE per la cibersicurezza (ENISA), il comitato per la valutazione della conformità e per la vigilanza del mercato nel settore delle telecomunicazioni e il gruppo europeo per la certificazione della cibersicurezza (ECCG) a partecipare attivamente a questa iniziativa volta a rafforzare il mercato unico digitale e ad accrescere la fiducia nei prodotti, servizi e processi TIC per i dispositivi connessi, garantendo la tutela della vita privata e la cibersicurezza, e ad agevolare una maggiore competitività globale del settore dell'internet delle cose dell'Unione garantendo i più elevati standard di resilienza, sicurezza e protezione;

17. SOTTOLINEA, in tale contesto, la necessità di sostenere le PMI quale componente essenziale dell'ecosistema europeo della cibersicurezza e INCORAGGIA le PMI a partecipare a tutte le consultazioni pubbliche avviate e alle attività di normazione, per tener conto del loro prezioso e importante contributo per rendere la cibersicurezza un obiettivo raggiungibile e un vantaggio competitivo sul mercato europeo;

18. RILEVA che l'obbligo di garantire la cibersicurezza e la tutela della vita privata lungo l'intero ciclo di vita di un prodotto e lungo tutta la sua catena di approvvigionamento potrebbe avere un impatto positivo sull'impronta ambientale del settore della tecnologia, orientando i fabbricanti verso processi di sviluppo e produzione intelligenti e sostenibili, riducendo in tal modo la quantità di rifiuti elettronici derivanti dallo smaltimento dei dispositivi connessi.