dossier

15 luglio 2021

Documentazione per le Commissioni

RIUNIONI INTERPARLAMENTARI

Riunione dei Presidenti della Conferenza degli organi parlamentari specializzati negli affari dell'Unione europea dei Parlamenti dell'Unione stessa (COSAC)

Videoconferenza, 19 luglio 2021

Senato della Repubblica

Camera dei deputati

XVIII LEGISLATURA

Senato della Repubblica

Camera dei deputati

XVIII LEGISLATURA

Documentazione per le Commissioni

RIUNIONI INTERPARLAMENTARI

Riunione dei Presidenti della Conferenza degli organi parlamentari specializzati negli affari dell'Unione europea dei Parlamenti dell'Unione stessa (COSAC)

Videoconferenza, 19 luglio 2021

SENATO DELLA REPUBBLICA
SERVIZIO STUDI
DOSSIER EUROPEI
N. 129

CAMERA DEI DEPUTATI
UFFICIO RAPPORTI CON
L'UNIONE EUROPEA
N. 64

Senato della Repubblica

Servizio Studi

TEL. 06 6706-2451 - studi1@senato.it - @SR_Studi

Dossier europei n. 129

Camera dei deputati

Ufficio rapporti con l'Unione europea

Tel. 06-6760-2145 - cdrue@camera.it

Dossier n. 64

INDICE

REPUBLIC OF SLOVENIA
NATIONAL ASSEMBLY
NATIONAL COUNCIL

Meeting of the Chairpersons of COSAC
19 July 2021, Ljubljana
Videoconference

Draft Programme (as of 14 July 2021)

MEETING TIME ZONE: CET

PARLEU2021.SI

Friday, 16 July 2021

10:00 - 11:00 **Meeting of the COSAC Presidential Troika**

Monday, 19 July 2021

9:00 - 9:20 **Opening of the meeting**

Welcome addresses:

- **Mr Igor Zorčič**, President of the National Assembly of the Republic of Slovenia
- **Mr Marko Pogačnik**, Chair of the Committee on EU Affairs of the National Assembly
- **Mr Bojan Kekec**, Chair of the Commission for International Relations and European Affairs of the National Council

Adoption of the Agenda of the COSAC Chairpersons' Meeting

9:20 - 9:45 **Procedural issues and miscellaneous matters**

- Results of the Meeting of the COSAC Presidential Troika
- Draft Programme of the LXVI COSAC Plenary Meeting
- Outline of the 36th Bi-annual Report of COSAC
- Letters received by the Presidency
- Information on the Appointment Process of the new Permanent Member of the COSAC Secretariat
- Other business

9:45 - 10:45 **SESSION I**

Priorities of the Slovenian Presidency of the Council of the European Union

Keynote Speaker:

- **Mr Anže Logar**, Minister of Foreign Affairs of the Republic of Slovenia

Debate

10:45 - 11:00 Break

11:00 - 12:30 **SESSION II**

Cybersecurity in the EU - Strengthening the Resilience of Critical Infrastructure and Cyber Defence

Keynote Speakers:

- **Mr Thierry Breton**, EU Commissioner for the Internal Market *(video message)*

- **Mr Matej Tonin**, Minister of Defence of the Republic of Slovenia
- **Mr Juhan Lepassaar**, Executive Director of the European Union Agency for Cybersecurity

Short intervention by:

- **Mr Uroš Svete**, Director of the Information Security Administration of the Republic of Slovenia

Debate

12:30 - 12:45 **Closing remarks by the Chairs**

I SESSIONE: PRIORITÀ DELLA PRESIDENZA SLOVENA DEL CONSIGLIO DELL'UE

La Slovenia ha assunto la Presidenza del Consiglio dell'UE del **secondo semestre del 2021** (dal **1° luglio al 31 dicembre 2021**). La Presidenza del Consiglio dell'UE è esercitata dal **Primo Ministro sloveno Ivan Janša**.

La Slovenia detiene la Presidenza del Consiglio dell'UE per la **seconda volta** (in precedenza l'aveva esercitata **nel primo semestre del 2008**), dopo essere entrata a far parte dell'UE il 1° maggio 2004.

Il **programma**, presentato ufficialmente il 1° luglio 2021, si articola in **quattro priorità**:

1. facilitare la **ripresa e rafforzare l'autonomia strategica e la resilienza dell'UE**;
2. riflettere sul **futuro dell'Europa**;
3. rafforzare lo **stato di diritto e i valori europei**;
4. aumentare la **sicurezza e la stabilità nel vicinato europeo.**

Le priorità della Presidenza slovena del Consiglio dell'UE sono state discusse nel corso dell'audizione dell'Ambasciatore di Slovenia in Italia, Tomaž Kunstelj, che si è svolta il 14 luglio 2021 presso le Commissioni riunite Affari esteri e Politiche dell'UE della Camera dei deputati.

1. Resilienza, ripresa e autonomia strategica dell'UE

Resilienza

Unione europea della salute

La Presidenza slovena pone l'accento sul rafforzamento dei sistemi sanitari e di altre infrastrutture critiche dell'UE e degli Stati membri e sull'importanza di potenziare la capacità di preparazione a future minacce sanitarie. In tale prospettiva intende sostenere l'iter delle proposte legislative che fanno parte del c.d. pacchetto dell'**Unione europea della salute**, presentato nel novembre 2020 (*si veda anche la comunicazione "Costruire un'Unione europea della salute: rafforzare la resilienza dell'UE alle minacce per la salute a carattere transfrontaliero" COM(2020)724*).

La prima proposta di regolamento, COM(2020)725, mira ad ampliare il ruolo dell'**Agenzia europea dei medicinali** (EMA) per favorire una risposta coordinata a livello dell'UE alle emergenze sanitarie mediante: *a)* il monitoraggio delle carenze di medicinali

e dispositivi medici essenziali; *b)* la consulenza scientifica per lo sviluppo di medicinali rivolti alla terapia, alla prevenzione o alla diagnosi delle patologie all'origine delle crisi; *c)* il coordinamento degli studi per valutare l'efficacia e la sicurezza dei vaccini; *d)* il coordinamento delle sperimentazioni cliniche. Il 15 giugno 2021 il Consiglio dell'UE ha raggiunto un accordo sul testo per il negoziato con il Parlamento, che ha votato la propria posizione in prima lettura l'8 luglio. Le restanti proposte, volte ad estendere le competenze **del Centro europeo per la prevenzione e il controllo delle malattie** (COM(2020)726) e ad aggiornare il quadro normativo esistente (si veda la decisione n. 1082/2013/UE) in materia di **gravi minacce per la salute a carattere transfrontaliero** (COM(2020)727), dovrebbero essere votate dal Parlamento europeo nella plenaria di settembre.

Il Senato ha esaminato le proposte legislative relative all'Unione europea della salute e la 14a Commissione (Politiche dell'Unione europea) ha approvato una risoluzione nella seduta del 12 maggio 2021 (Doc. XVIII-*bis* n. 9).

Il programma annuncia l'organizzazione nel mese di luglio di una conferenza di alto livello sulla resilienza dei sistemi sanitari.

Resilienza agli attacchi informatici

In tale ambito la Presidenza slovena si impegna altresì a rafforzare la resilienza agli attacchi informatici, ponendo l'accento sulla protezione delle **infrastrutture critiche** e del **mercato unico digitale**.

In particolare, viene sottolineato l'obiettivo di compiere progressi decisivi per quanto riguarda la proposta (COM(2020)823) volta a sostituire la cd. direttiva NIS, recante un quadro di obblighi a carico di soggetti **pubblici** e **privati** che svolgono funzioni essenziali per l'economia e la società nel campo della sicurezza cibernetica.

Il nuovo regime verte sui seguenti pilastri: 1) capacità degli Stati Membri in termini di architettura istituzionale, **strategia nazionale** e **piani** di gestione delle crisi cibernetiche; 2) gestione del **rischio** da parte degli operatori, con **misure** di sicurezza adeguate e un sistema di **notifica** di incidenti efficace e reattivo; 3) **cooperazione** e **condivisione** di **informazioni**, prevedendo diversi sistemi di **collegamento** tra il livello europeo e nazionale.

La riforma sulla protezione dei **soggetti critici** (COM(2020)829), all'esame dei colegislatori europei, estenderebbe sia l'ambito di applicazione, sia la profondità della direttiva sulle infrastrutture critiche europee del 2008, contemplando i seguenti settori: energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio. Ciascuno Stato membro dovrebbe adottare una strategia nazionale per garantire la resilienza dei soggetti critici ed effettuerebbe valutazioni periodiche dei rischi, al fine di individuare un sottoinsieme più ristretto di soggetti critici cui incomberebbero obblighi volti a rafforzarne la loro sicurezza di fronte ai rischi non informatici, comprese le valutazioni dei rischi a livello di soggetto, l'adozione di misure tecniche e organizzative e la notifica degli incidenti.

Autonomia strategica

Strategia industriale aggiornata dell'UE

La Presidenza slovena intende dedicare particolare attenzione all'**attuazione della strategia industriale aggiornata** dell'UE, che comprende anche il rafforzamento dell'autonomia strategica e della sovranità tecnologica dell'UE.

Si ricorda che la strategia industriale aggiornata (COM(2021)350) è stata presentata dalla Commissione il 5 maggio 2021. Essa intende, in particolare, rafforzare la resilienza del mercato unico, in modo da garantire la libera circolazione di beni, servizi e lavoratori anche in tempi di crisi, ridurre le dipendenze dell'Unione in settori tecnologici e industriali strategici essenziali (autonomia strategica aperta) e accelerare la duplice transizione verde e digitale.

La Presidenza intende anche avviare un dibattito sulle misure a tutela del mercato interno e degli investimenti strategici, al fine di rafforzare la sostenibilità delle catene del valore europee, e impegnarsi per una politica commerciale aperta, contrastando al contempo le pratiche commerciali sleali. Intende altresì intensificare il dibattito sulla gestione del traffico spaziale per garantire la sicurezza e l'autonomia dell'industria spaziale europea.

Autorità europea per la preparazione e la risposta alle emergenze sanitarie (HERA)

Un importante elemento dell'autonomia strategica dell'UE è l'autosufficienza nel settore farmaceutico e dei vaccini. Nel corso della Presidenza slovena dovrebbe essere avviata la discussione sulla proposta, di prossima presentazione, per l'istituzione della nuova **Autorità europea per la preparazione e la risposta alle emergenze sanitarie** (**HERA**), che dovrebbe tra l'altro monitorare fabbisogni e disponibilità di materie prime per garantire l'adeguatezza della produzione e delle catene di approvvigionamento di medicinali e dispositivi medici. Obiettivo dichiarato nel programma della Presidenza slovena è che HERA abbia una propria ricerca e capacità di sviluppo nonché adeguate infrastrutture per la produzione di medicinali e vaccini.

L'iniziativa legislativa è stata preceduta da un piano di preparazione alla bio-difesa contro la COVID-19, denominato "**incubatore HERA**" (COM(2021)78), volto a contrastare la diffusione delle varianti del Sars-Cov-2 tramite il potenziamento del **sequenziamento** genomico e incentivi per l'aggiornamento dei vaccini.

Infrastrutture energetiche (TEN-E)

Al fine di migliorare l'integrazione delle infrastrutture energetiche e garantire la sicurezza dell'approvvigionamento, la Presidenza slovena intende inoltre accordare priorità all'iter della proposta di revisione del regolamento sulle **infrastrutture energetiche (TEN-E)** (COM(2020)824, tuttora all'esame del Parlamento europeo) per aggiornarlo al processo di decarbonizzazione a lungo termine dell'Unione europea.

Approvvigionamento alimentare

Infine, la Presidenza slovena ricorda l'importanza strategica dell'**approvvigionamento alimentare nell'UE**, secondo quanto stabilito anche dalla strategia Farm to Fork. Secondo il programma, infatti, uno degli obiettivi della Presidenza slovena sarà quello di favorire lo sviluppo di una filiera alimentare sicura, adeguata, sostenibile e resiliente, anche nell'ottica di perseguire un generale miglioramento del sistema di gestione delle crisi dell'UE.

Ripresa

Piani nazionali per la ripresa e la resilienza

Una priorità della Presidenza slovena sarà l'effettiva attuazione del bilancio pluriennale dell'UE 2021-2027 e dello strumento *Next Generation EU*, con particolare attenzione alla rapida adozione dei **Piani nazionali per ripresa e la resilienza**.

Sulla base delle informazioni che si possono ricavare dal sito della Commissione europea sono stati ufficialmente **trasmessi 25 Piani nazionali** (non risultano ancora trasmessi i Piani di Bulgaria e Paesi Bassi).

La Commissione europea ha già adottato una **valutazione positiva** per i Piani di Austria, Belgio, Cipro, Croazia, Danimarca, Francia, Germania, Grecia, **Italia**, Lettonia, Lituania, Lussemburgo, Portogallo, Slovacchia, Slovenia e Spagna.

Il **13 luglio 2021** il **Consiglio** "Economia e finanza" (**ECOFIN**) ha **approvato** i Piani di Austria, Belgio, Danimarca, Francia, Germania, Grecia, **Italia**, Lettonia, Lussemburgo, Portogallo, Slovacchia e Spagna.

Nuove risorse proprie dell'UE

Inoltre, la Presidenza slovena intende favorire il dibattito circa l'introduzione di **nuove risorse proprie**, al fine di alleviare gli oneri per i bilanci degli Stati membri e creare uno spazio fiscale che permetta l'indirizzamento delle risorse verso la ripresa economica. In particolare, la

Presidenza intende impegnarsi per esaminare una proposta per la tassazione digitale e una nuova risorsa propria basata su un meccanismo di adeguamento del carbonio alle frontiere.

Si ricorda che le istituzioni europee (Accordo interistituzionale del 16 dicembre 2020) si sono accordate per una **tabella di marcia** per l'introduzione di **nuove risorse proprie** che potrebbero essere, tra l'altro, **utilizzate per il rimborso anticipato dei prestiti** contratti a titolo di *Next Generation EU*. Le istituzioni europee riconoscono che le nuove risorse proprie dovrebbero ridurre la quota dei contributi nazionali basati sul reddito nazionale loro (RNL) e sostenere le priorità dell'Unione, come il *Green Deal* europeo e il digitale, nonché contribuire all'equità fiscale e al rafforzamento della lotta contro la frode e l'evasione fiscali.

La tabella di marcia specifica le seguenti tappe:1) **Prima tappa**: **2021**: viene introdotto, a decorrere dal 1° gennaio 2021, un contributo degli Stati membri basato sui rifiuti di imballaggio di plastica non riciclati. Inoltre, la Commissione europea deve presentare proposte relative a un meccanismo di adeguamento del carbonio alla frontiera e a un prelievo sul digitale in vista della loro introduzione al più tardi il 1° gennaio 2023. Deve altresì riesaminare il sistema di scambio di quote di emissione dell'UE, considerandone anche la possibile estensione ai settori dell'aviazione e marittimo e proporre una risorsa propria basata sul sistema di scambio di quote di emissione; 2) **Seconda tappa**: **2022 e 2023**: il Consiglio delibererà in merito a queste nuove risorse proprie al più tardi entro il 1° luglio 2022 in vista della loro introduzione entro il 1° gennaio 2023; 3) **Terza tappa**: **2024-2026**: la Commissione europea proporrà nuove risorse proprie supplementari che potrebbero comprendere un'imposta sulle transazioni finanziarie e un contributo finanziario collegato al settore societario o una nuova base imponibile comune per l'imposta sulle società. La Commissione si adopererà per presentare una proposta **entro giugno 2024**. Il Consiglio delibererà in merito a queste nuove risorse proprie al più tardi entro il 1° luglio 2025 in vista della loro introduzione entro il 1° gennaio 2026.

Si segnala che la proposta di regolamento che istituisce un meccanismo di adeguamento del carbonio alle frontiere (COM(2021)564 - testo in inglese) è stata presentata dalla Commissione il 14 luglio 2021.

La Presidenza slovena, al fine di tutelare l'efficienza a lungo termine del sistema finanziario, annuncia altresì che intende promuovere il dibattito sull'attuazione di **regole di bilancio** dell'UE che possano garantire l'equilibrio tra il sostegno fornito alla crescita e la stabilità di bilancio a lungo termine.

Green Deal

La Presidenza slovena intende altresì lavorare per recepire gli **obiettivi ambientali e climatici** fissati dal *Green Deal* e dalla **legge europea sul clima,** recentemente approvata (il testo è stato votato il 24 giugno 2021 dal Parlamento europeo e adottato dal Consiglio il 28 giugno): la **neutralità**

climatica entro il 2050 e la **riduzione delle emissioni** di gas serra di almeno il **55% entro il 2030**, rispetto al 1990.

La 13a Commissione (Territorio, ambiente, beni ambientali) aveva approvato una risoluzione sulla proposta della Commissione nella seduta del 22 gennaio 2021 (Doc. XVIII n. 21).

In tale prospettiva il programma assegna priorità al pacchetto di proposte legislative, c.d. "**Fit for 55**", che la Commissione europea si appresta a presentare per il raggiungimento del *target* 2030.

Tra le misure, che dovrebbero essere presentate entro luglio, figurano l'introduzione di un meccanismo di **adeguamento del carbonio alle frontiere**, una proposta per la riduzione delle emissioni di **metano** nel settore dell'energia e la revisione:

- del sistema di **scambio di quote di emissioni** dell'UE (*Emission Trading Scheme* - ETS);
- dei regolamenti sulla **condivisione degli sforzi** (*Effort sharing regulation* - ESR) e sull'inclusione delle emissioni e degli assorbimenti di gas ad effetto serra risultanti dall'**uso del suolo**, dal cambiamento di uso del suolo e dalla silvicoltura (*Land use, land use change and forestry* - LULUCF);
- delle direttive in materia di **energie rinnovabili**, **efficienza energetica,** e sulla realizzazione di un'infrastruttura per i **combustibili alternativi**.

A queste si aggiungeranno la revisione della direttiva in materia di **prestazione energetica nell'edilizia**, e del terzo "pacchetto energia" sul gas, per la regolamentazione e la competitività di **mercati del gas decarbonizzati**, che dovrebbero essere presentate in autunno.

La Presidenza annuncia l'intenzione di avviare i negoziati sulle nuove proposte della Commissione alla luce dei principi di **solidarietà**, **equità** ed **economicità**, e nel rispetto del diritto degli Stati membri di scegliere **mix energetico** e tecnologie, inclusa la possibilità di sfruttare il potenziale dell'energia nucleare sicura.

Nel programma si ricorda che il settore dei trasporti è una fonte significativa di gas ad effetto serra e che il *Green Deal* prevede in questo ambito una riduzione delle emissioni del 90% entro il 2050. La presidenza slovena intende dare centralità al tema della **mobilità sostenibile** e **intelligente**, all'aggiornamento della **rete transeuropea TEN-T** e allo sviluppo e alla diffusione di **combustibili alternativi**. Un'importanza strategica è attribuita alla **mobilità elettrica** a basse emissioni, all'infrastrutturazione per la ricarica dei veicoli elettrici, e ad un più ampio ricorso al trasporto ferroviario. La Presidenza intende pertanto avviare i negoziati sulla prossima proposta per la revisione della direttiva

sull'infrastruttura dei carburanti alternativi (vedi *supra*) e sostenere le iniziative per il 2021 come Anno europeo delle ferrovie.

La Commissione dovrebbe presentare nella seconda parte dell'anno una proposta per la revisione della rete transeuropea TEN-T, su cui ha già svolto una consultazione pubblica, conclusa il 5 maggio 2021. Sullo stesso tema il Parlamento europeo ha approvato una risoluzione non legislativa il 20 gennaio 2021.

Inoltre, secondo la Presidenza slovena l'istituzione di una **norma UE per le obbligazioni verdi** potrebbe contribuire al raggiungimento degli obiettivi climatici.

La proposta di regolamento (COM(2021)391) su una norma europea per le obbligazioni verdi (EUGBS, *European Green Bond Standard*), che introdurrà uno standard rigoroso a cui tutti gli emittenti (privati e sovrani) potranno aderire volontariamente, è stata presentata il 6 luglio 2021.

Le politiche per il clima saranno centrali nel semestre sloveno, anche per la preparazione della **Conferenza delle Parti sul cambiamento climatico delle Nazioni Unite** (COP26), che si terrà a Glasgow il prossimo novembre con la presidenza del Regno Unito in partenariato con l'Italia. La posizione dell'UE sarà definita in Consiglio nel mese di ottobre e la Presidenza slovena, che rappresenterà l'UE, si dichiara orientata a costruire consenso su un mandato che consenta all'Unione di assumere un ruolo *leader* e che contribuisca al completamento del **quadro di regole** per **l'attuazione dell'accordo di Parigi**.

In vista della Conferenza, il Consiglio europeo, nella riunione del 24 e 25 maggio 2021, ha già invitato i partner internazionali, in particolare i membri del G20, a innalzare il livello di ambizione delle politiche sul clima. La commissione Ambiente del Parlamento europeo ha cominciato a discutere una bozza di risoluzione sulla partecipazione alla **COP26** che dovrebbe essere votata dalla plenaria a ottobre e in cui si invitano le parti a migliorare **i contributi determinati a livello nazionale** (**NDC**, *nationally determined contributions*), attualmente non sufficienti a raggiungere gli obiettivi dell'accordo di Parigi, e si invitano in particolare le nazioni del G20 a prefiggersi il conseguimento della neutralità climatica entro il 2050.

La Presidenza sottolinea l'importanza di realizzare un'**economia circolare** e di adottare **tecnologie innovative** per contribuire alla transizione climatica, salvaguardare la competitività delle imprese e ridurre la dipendenza dell'Unione nell'approvvigionamento di materie prime critiche. In particolare, dichiara l'intenzione di raggiungere un accordo su un orientamento generale sulla proposta di regolamento sulle **batterie.**

Il testo (COM(2020)798), tuttora all'esame del Parlamento europeo, è volto ad armonizzare ed aggiornare la normativa vigente per incentivare nell'Unione la produzione

di batterie sostenibili, lo smaltimento, il riciclo e l'adeguato trattamento delle sostanze pericolose.

La Presidenza prevede inoltre di avviare la discussione sulla proposta di revisione del regolamento sulla **spedizione dei rifiuti**, che la Commissione dovrebbe presentare nella seconda parte dell'anno. Le nuove norme dovrebbero ridurre le esportazioni verso paesi terzi di rifiuti, che causano danni all'ambiente o alla salute umana, contrastare i comportamenti illeciti e garantire che il trattamento dei rifiuti avvenga in modo trasparente e tracciabile e secondo i principi dell'economia circolare.

Politica agricola comune

Inoltre, la Presidenza slovena annuncia che sta pianificando un **dibattito politico sulla preparazione dei piani strategici per l'attuazione della politica agricola comune** e che parteciperà attivamente alla conferenza "Farm to Fork", che si terrà ad ottobre in occasione della Giornata mondiale dell'alimentazione. Infine, sulla base della rinnovata strategia forestale dell'UE post-2020, la Presidenza slovena annuncia che intensificherà il dibattito sulla gestione forestale integrata, sottolineando l'importanza della gestione forestale sostenibile.

Transizione digitale

Secondo la Presidenza slovena, nel processo di **trasformazione digitale** sono necessari progressi nella **regolamentazione dei servizi e dei mercati digitali** con i quali l'UE creerà nuovi standard nell'uso delle piattaforme digitali.

Sono tuttora all'esame dei colegislatori europei i cosiddetti ***Digital services act*** (COM(2020)825) e ***Digital markets act*** (COM(2020)842), volti, rispettivamente, a stabilire una **disciplina orizzontale** sulle condizioni di fornitura di beni, servizi e contenuti *online* (che integrerebbe e sostituirebbe parzialmente la vigente direttiva *e-commerce*), e ad assicurare un **mercato digitale equo e contendibile**, stabilendo, in particolare, una serie di **obblighi e divieti a carico delle piattaforme di intermediazione *online*** così grandi da assumere il ruolo di cosiddetto *gatekeeper*, controllori dell'accesso nell'ecosistema digitale. Le proposte sono state esaminate dalla IX Commissione (Trasporti) della Camera dei deputati, che, il 23 giugno 2021, ha adottato in merito due distinti documenti finali.

Nell'ambito dei Consigli dedicati alle telecomunicazioni ulteriori dossier prioritari della Presidenza slovena dovrebbe essere rappresentati, tra l'altro, dai seguenti:

- il *Data governance act* (COM(2020)767) che mira a promuovere la messa a disposizione dei **dati** del settore pubblico per il riutilizzo

qualora tali dati siano oggetto di diritti di terzi e la condivisione dei dati tra le imprese, dietro compenso in qualsiasi forma;

- il primo quadro giuridico sull'**intelligenza artificiale** (COM(2021)206) con l'obiettivo di valutare i rischi connessi all'impiego di tale tecnologia, e di salvaguardare nell'ambito di tale utilizzo i valori e i diritti fondamentali dell'UE e la sicurezza degli utenti;
- la riforma del regolamento n. 910/2014 in materia di **identificazione elettronica** e servizi fiduciari per le transazioni elettroniche nel mercato interno;
- la revisione delle norme in materia di tutela della vita privata e della riservatezza nell'uso di servizi di comunicazione elettronica.

Si ricorda, in particolare, il quadro giuridico volto ad assicurare che i sistemi di **intelligenza artificiale** (IA) immessi sul mercato dell'Unione siano sicuri e rispettino la normativa vigente in materia di **diritti fondamentali** e i valori dell'Unione. Il nuovo regime stabilisce un elenco di **pratiche** di IA **vietate**, seguendo un approccio basato sul **rischio** connesso ai differenti usi di tale tecnologia. Il *Governance data act* mira a promuovere la disponibilità dei dati rafforzando i meccanismi di condivisione di informazione in tutta l'UE e ad accrescere la fiducia negli intermediari che agiranno nei diversi spazi di dati.

La Presidenza slovena intende anche favorire la discussione sulle proposte legislative in materia di **finanza digitale**.

Si segnala che è in corso di esame, al Senato della Repubblica presso la 6ª Commissione permanente (Finanze e tesoro) e alla Camera dei deputati presso la VI Commissione (Finanze), un **pacchetto di misure in materia di finanza digitale**, presentato dalla Commissione europea lo scorso settembre, contenente tra l'altro un quadro generale dell'Unione in materia di **cripto-attività**, un'ulteriore armonizzazione delle principali prescrizioni sulla resilienza operativa digitale e una strategia in materia di pagamenti al dettaglio. Per approfondimenti, si vedano il dossier predisposto dal Servizio Studi del Senato e il dossier predisposto dall'Ufficio Rapporti con l'Unione europea della Camera dei deputati.

Particolare attenzione è infine dedicata nel Programma della Presidenza slovena all'attuazione della nuova **strategia** dell'**UE** per la **cibersicurezza**, e all'implementazione del *Cibersecurity act*, nonché degli strumenti volti a garantire la sicurezza dell'**infrastruttura 5G**, e la sicurezza dei dispositivi collegati a Internet. Il tema è peraltro approfondito anche nella parte del Programma relativo alle misure per la **resilienza**, nel cui contesto la Presidenza slovena dichiara l'intenzione di sostenere la **sicurezza informatica** e il rafforzamento delle capacità nei paesi dei **Balcani occidentali**, a causa dell'elevato livello di esposizione dell'UE alle minacce

informatiche che si possono verificare nell'immediato vicinato. A tal proposito il programma prevede che ai margini del **Forum strategico di Bled**, che dovrebbe svolgersi all'inizio di settembre 2021, si organizzi una **conferenza di alto livello sulla sicurezza informatica** cui invitare anche rappresentanti dei **Balcani occidentali**.

Mercato unico

Il programma fa riferimento anche alla necessità di **approfondire il mercato unico**, in particolare rimuovendo le barriere transfrontaliere ai servizi e alla libera circolazione di merci e persone e aggiornando le norme a protezione dei consumatori e le norme sugli aiuti di Stato.

Turismo

Il programma attribuisce un ruolo centrale anche al sostegno delle attività maggiormente colpite dall'emergenza COVID-19, come il **turismo**, anche per sostenerne la capacità di affrontare eventuali crisi future. In questa prospettiva la Presidenza slovena è orientata ad avviare una discussione sulle sfide e le opportunità di un'industria del turismo in grado di recuperare competitività integrandosi nella transizione climatica e digitale. Su questi temi la Slovenia promuoverà un dibattito tra i ministri del turismo dell'UE e al **Forum Europeo del Turismo 2021**, che la Slovenia sta organizzando in cooperazione con la Commissione europea e che si svolgerà il 17 novembre 2021 a Brdo.

Ricerca e innovazione

La Presidenza slovena sottolinea, inoltre, il **ruolo della scienza e della ricerca** per conseguire la ripresa economica e un'efficace transizione verde e digitale: intende, in particolare, lavorare per potenziare lo Spazio europeo della ricerca (ERA), promuovere nuovi approcci, come le missioni all'interno di Orizzonte Europa (il nuovo programma quadro dell'UE 2021-2027 per la ricerca e l'innovazione) e il Nuovo Bauhaus Europeo, adottare, a livello di Consiglio dell'UE, il Patto per la Ricerca e l'Innovazione, e organizzare, a ottobre a Lubiana, una conferenza di alto livello sul ruolo della ricerca e dell'innovazione nell'UE e sui compiti della ricerca europea.

Questione demografica e dimensione sociale

La Presidenza slovena evidenzia altresì la necessità di **affrontare la questione demografica**, ritenendolo un elemento essenziale per la ripresa,

con l'obiettivo di promuovere politiche di alta qualità che contribuiscano a invertire le tendenze demografiche negative. In particolare, la Presidenza annuncia l'organizzazione, a ottobre, di una conferenza ad alto livello sul lavoro di qualità per promuovere cambiamenti nell'equilibrio tra vita professionale e familiare, l'acquisizione permanente di abilità e conoscenze e la salute e la sicurezza sui luoghi di lavoro, tenendo conto anche della digitalizzazione nel mondo del lavoro.

Infine, la Presidenza slovena ribadisce che il **Pilastro europeo dei diritti sociali** è fondamentale per gestire le attuali sfide sociali ed economiche nell'UE.

Il **4 marzo 2021** la Commissione europea ha presentato il **Piano d'azione** sul Pilastro europeo dei diritti sociali (COM(2021)102 e allegati). Esso delinea le azioni, legislative e non, che la Commissione intende adottare, durante il suo mandato (entro la fine del 2024), per proseguire l'attuazione dei venti principi del Pilastro europeo dei diritti sociali e propone **tre obiettivi principali** in materia di occupazione, competenze e protezione sociale che **l'UE** deve conseguire **entro il 2030**, in linea con gli obiettivi di sviluppo sostenibile delle Nazioni Unite: 1) **almeno il 78%** della **popolazione** di età compresa **tra i 20 e i 64 anni** dovrebbe avere un lavoro; 2) almeno **il 60%** degli **adulti** dovrebbe partecipare **ogni anno** ad **attività di formazione**; 3) **ridurre di almeno 15 milioni il numero di persone a rischio di povertà o di esclusione sociale** (5 milioni dei quali dovrebbero essere bambini).

2. Conferenza sul Futuro dell'Europa

La Presidenza intende **incoraggiare il dibattito sul futuro comune dell'Europa,** in considerazione delle numerose sfide che l'UE ha dovuto affrontare negli ultimi anni e delle aspettative dei cittadini

La Presidenza intende dedicare **particolare attenzione** a questo dibattito in seno alla **Conferenza sul futuro dell'Europa** ed assicurare che il **Consiglio dell'UE e gli Stati membri vi svolgano un ruolo appropriato**.

La Presidenza indica che nell'ambito del suo semestre contribuirà all'organizzazione di due riunioni dell'Assemblea plenaria della Conferenza (previste il **22 e 23 ottobre 2021** e il **17 e 18 dicembre 2021**) e vari panel europei dei cittadini, assicurando che le idee e proposte formulate dai cittadini in tali sedi siano adeguatamente rappresentate nelle riunioni delle Assemblea plenaria della Conferenza.

La Presidenza slovena si impegna, inoltre, ad i**nformare regolarmente il Consiglio dell'UE sui lavori della Conferenza** ed affinché essi

progrediscano come stabilito, con **l'obiettivo della sua conclusione per la primavera del 2022**, nell'arco del semestre della presidenza di turno della Francia.

La Presidenza slovena farà ogni sforzo per **assicurare che tutte le differenti legittime visioni sul futuro dell'Europa siano tenute in considerazione** ed indica come proprio **obiettivo** quello di rafforzare la comprensione comune che **alcune sfide possono essere affrontate solo a livello europeo**, **mentre per altre è più facile per gli Stati membri operare in proprio con la necessaria autonomia** pur nella cornice europea.

A tal fine, la Presidenza slovena annuncia che ai **primi di settembre 2021** dedicherà il ***16° Bled Strategic Forum*** ad un dibattito sul futuro dell'Europa, al quale saranno invitati i più importanti attuali leader europei e che intende, inoltre, organizzare un panel di discussione, con la partecipazione dei più importanti leader europei del passato, sulle opportunità che l'UE non è stata capace di realizzare.

Il **Bled Strategic Forum** è una **conferenza internazionale annuale** organizzata dal 2006 a Bled in Slovenia, e il cui scopo è quello di stimolare una discussione su opinioni contrastanti sulla società moderna e sul suo futuro.

Si ricorda che la **Conferenza sul futuro dell'Europa** è stata inaugurata il **9 maggio 2021**, in occasione della Giornata dell'Europa, a Strasburgo nella sede del Parlamento europeo e il **19 giugno 2021**, sempre a Strasburgo si è svolta, in formato ibrido, la **prima sessione plenaria della Conferenza sul futuro dell'Europa**, l'iniziativa volta a coinvolgere cittadini di ogni categoria, rappresentanti della società civile, istituzioni europee, nazionali, regionali e locali in una riflessione congiunta sulle politiche e sulle ambizioni dell'UE. Questa riflessione collettiva si svolgerà attraverso **iniziative di consultazione e dibattiti a livello decentrato** (anche attraverso una piattaforma multilingue digitale), i cui risultati saranno discussi in sede plenaria.

A tal fine, a **partire dal settembre 2021**, si svolgeranno le **riunioni dei 4 panel europei dei cittadini** dedicati rispettivamente a: 1) **democrazia / valori europei, diritti, Stato di diritto, sicurezza**; 2) **cambiamento climatico, ambiente e salute**; 3) **economia più forte, giustizia sociale, lavoro, istruzione, gioventù, cultura, sport, trasformazione digitale**; 4) **l'UE nel mondo / migrazione**. Ad ogni *panel* potranno partecipare **200 cittadini degli Stati membri dell'UE** con la stessa ripartizione degressivamente proporzionale prevista per la composizione del Parlamento europeo e **un terzo** di ogni panel sarà costituito da **giovani tra 16 e 25 anni**. I panel europei dei cittadini avranno il compito di **formulare delle raccomandazioni** che saranno **discusse dall'Assemblea plenaria della Conferenza**.

Secondo il calendario dei lavori della Conferenza, **per ogni panel sono previste 3 distinte sessioni di lavoro** di 3 giorni ciascuna che si svolgeranno **per la quasi totalità nel corso della Presidenza slovena**.

3. Stato di diritto e i valori europei

La Presidenza slovena intende prestare particolare attenzione al rispetto per i **valori fondamentali** e i **principi** dell'UE, tra cui lo Stato di diritto, che è corresponsabilità delle Istituzioni UE e degli Stati membri. In particolare, nel programma si sottolineano i temi della **libertà** e del **pluralismo** dei media, del contrasto alle *fake news* e del corretto funzionamento dei **sistemi giudiziari**.

In proposito, il programma annuncia l'organizzazione di una **Conferenza internazionale** da svolgersi il 23 agosto 2021 in Slovenia, in occasione della Giornata europea del ricordo per le **vittime** dei **totalitarismi**.

La Presidenza slovena in ogni caso ritiene che una buona comprensione delle caratteristiche costituzionali socio-economiche, politiche, storiche, nonché delle **similitudini** e delle **differenze** tra Stati membri, possa contribuire a rafforzare lo Stato di diritto nell'UE. Inoltre, il programma pone l'accento sulla necessità di approfondire il dibattito sullo Stato di diritto secondo un approccio giuridico, **depoliticizzando** il più possibile la discussione e garantendo un trattamento equo dei diversi sistemi costituzionali e delle diverse pratiche nei rispettivi Stati membri. In particolare, la Presidenza slovena ritiene che il **meccanismo** sullo Stato di diritto debba operare in modo **obiettivo** e **trasparente**, nel rispetto dell'**uguaglianza** degli Stati membri, e delle **identità nazionali**. A tal proposito, la Presidenza è convinta che potrebbe offrire un contributo al consolidamento dello Stato di diritto l'istituzione di una **fondazione europea** per la democrazia costituzionale, composta da esperti, con il mandato di predisporre analisi e approfondimenti autonomi e indipendenti. La Presidenza si dice disposta ad ospitare l'*head office* di tale fondazione e a sostenerne le **infrastrutture** di base per il suo funzionamento.

Da ultimo sulla base della relazione annuale della Commissione europea, la Presidenza slovena intende condurre un dialogo annuale sulla situazione dello Stato di diritto nell'UE e nei singoli Stati membri, con l'obiettivo di promuovere una cultura dello Stato di diritto in tutta l'UE e, attraverso un dibattito inclusivo, consentire agli Stati membri di imparare dalle reciproche esperienze.

Nell'ambito del meccanismo per lo Stato di diritto, la Commissione europea ha presentato la prima Relazione sullo Stato di diritto 2020 - La situazione dello Stato di diritto nell'Unione europea, comprensiva dei capitoli per Stato membro, nel settembre del 2020.

Il documento è all'esame delle Commissioni congiunte I (Affari costituzionali) e II (Giustizia) della Camera. Secondo fonti informali la seconda Relazione sullo Stato di diritto dovrebbe essere presentata nel luglio 2021.

Si ricorda infine che nell'ambito dei Consigli dedicati alla giustizia, la Presidenza slovena intende prestare particolare attenzione alle politiche di contrasto dei **reati** e dei **discorsi** di **odio**, nonché al processo di **digitalizzazione** della giustizia. Ulteriore dossier prioritario dovrebbe essere costituito dal processo di adesione dell'UE alla **Convenzione europea dei diritti dell'uomo** (CEDU).

Circa le politiche di contrasto dei reati e dei discorsi di odio, merita segnalare che nel dicembre 2020 il Consiglio dell'UE ha approvato una dichiarazione sull'integrazione della **lotta** contro l'**antisemitismo** in tutti i settori d'intervento.

Da ultimo si ricorda che l'art. 6, par. 2, del Trattato sull'Unione europea prevede l'**adesione dell'UE alla CEDU**, precisando che tale adesione non modifica le competenze dell'Unione definite dai Trattati. In virtù dell'adesione, la CEDU, come avviene per qualsiasi altro **accordo internazionale** concluso dall'Unione, vincolerebbe le istituzioni di quest'ultima e gli Stati membri, formando parte integrante del diritto dell'Unione. L'Unione sarebbe sottoposta, al pari di qualsiasi altra parte contraente, ad un **controllo esterno** avente ad oggetto il rispetto dei diritti e delle libertà previsti dalla CEDU, ed in particolare alle decisioni della **Corte europea dei diritti dell'uomo**. La CEDU contiene una serie di **diritti** e **libertà fondamentali** (diritto alla vita, divieto della tortura, divieto della schiavitù e del lavoro forzato, diritto alla libertà ed alla sicurezza, diritto ad un processo equo, principio di legalità, diritto al rispetto della vita privata e familiare, libertà di pensiero, di coscienza e di religione, libertà d'espressione, libertà di riunione e d'associazione, diritto al matrimonio, diritto ad un ricorso effettivo, divieto di discriminazione).

Successivamente a una fase di stallo, sostanzialmente dovuta al parere negativo della Corte di giustizia dell'UE sulla prima bozza di accordo, il Consiglio dell'UE ha promosso una ripresa dei negoziati.

La Presidenza slovena intende inoltre richiamare l'attenzione sulla necessità di **contrastare le tendenze demografiche negative nell'UE**.

Si ricorda che in base alla relazione demografica della Commissione europea, nell'UE:

- nel 2018, la **speranza di vita** alla nascita è salita a **78,2 anni** per gli **uomini** e a **83,7** anni per le **donne**. Si prevede che questa tendenza continuerà: gli uomini nati nel **2070** dovrebbero vivere fino a **86 anni** e le donne fino a **90 anni**;
- nel 2018, il numero medio di **figli** per donna era di 1,55 e l'età media al momento del parto era di 31,3 anni;

- entro il **2070** il **30,3** per cento della popolazione dovrebbe avere almeno **65 anni** (rispetto al 20,3 per cento nel 2019) e il **13,2** per cento dovrebbe avere almeno **80 anni** (rispetto al 5,8 **per cento** nel 2019),
- la quota della popolazione europea sta **calando** rispetto a quella **mondiale** e nel 2070 rappresenterà poco meno del **4 per cento**.

4. Aumentare la sicurezza e la stabilità del vicinato europeo

La Presidenza slovena intende:

- promuovere, sostenendo l'operato dell'Alto rappresentante per la politica estera e di sicurezza comune, il **rafforzamento delle relazioni transatlantiche**, attraverso una stretta cooperazione con gli Stati Uniti e con la NATO basata su principi, valori e interessi comuni. In particolare, la Presidenza slovena intende **promuovere la consapevolezza che la cooperazione con gli Stati Uniti come un alleato strategico chiave** è **essenziale per il successo delle attività dell'UE nel vicinato europeo,** nonché nelle questioni di importanza globale, come la **lotta al cambiamento climatico e il contrasto alle minacce informatiche e ibride**;
- dedicare particolare attenzione ai paesi dei **Balcani occidentali**, al loro futuro in Europa e alla credibile continuazione del processo di allargamento dell'UE. In particolare, la Presidenza intende impegnarsi per la **ripresa economica** dei paesi della regione, promuovendo la **transizione verde e digitale**, migliorando la connettività all'interno della regione e con l'Unione europea e rafforzando la resilienza della regione, compresa la sua resilienza informatica. Ad **ottobre 2021** la Presidenza ha in programma lo svolgimento di un **vertice UE-Balcani occidentali**; inoltre, la Presidenza slovena intende **avanzare nel dialogo Belgrado-Pristina** e **includere i paesi partner dei Balcani nelle iniziative di politica di sicurezza e di difesa comune dell'UE**.

  Si ricorda che l'**adozione dei mandati** per l'avvio dei negoziati con l'**Albania** e la **Macedonia del Nord** è **ancora bloccata in seno al Consiglio dell'UE** (che li deve approvare all'unanimità) per **il veto espresso dalla Bulgaria**, che condiziona il suo assenso al riconoscimento da parte della Macedonia del Nord di condizioni relative al retaggio storico e linguistico comune. La Presidenza portoghese puntava a raggiungere un accordo per l'avvio dei negoziati entro la conclusione del suo semestre di Presidenza (30 giugno 2021). A causa del persistere del veto della Bulgaria la **decisione** da parte del Consiglio è stata **rinviata** alla **Presidenza slovena.** Per quanto riguarda gli altri paesi dei Balcani occidentali coinvolti nel

processo di allargamento, la **Serbia** ha **avviato i negoziati di adesione nel gennaio 2014**, nell'ambito dei quali sono stati **aperti 18 capitoli** negoziali (sui 34 totali), di cui 2 sono stati chiusi (Scienza e ricerca; Educazione e cultura), e la **Bosnia-Erzegovina** e il **Kosovo** sono qualificati come "**potenziali candidati**", anche se solo la prima ha presentato domanda di adesione il 15 febbraio 2016;

- promuovere un **ampio dibattito sulla politica europea di vicinato**, con riferimento sia alla **dimensione meridionale** che a quella **orientale**, in particolare, promuovendo l'attuazione della **nuova agenda per il Mediterraneo**, in vista della sua discussione da parte del Consiglio europeo del dicembre 2021 e definendo gli obiettivi per la cooperazione con i paesi partner orientali, in vista del **Vertice UE sul partenariato orientale** che si svolgerà a **Bruxelles nell'ottobre 2021**;

  Si ricorda che la **Commissione europea e l'Alto rappresentante** hanno presentato il **9 febbraio 2021** una **comunicazione congiunta** nella quale si propone di avviare una **nuova Agenda per il Mediterraneo**, accompagnata da un **piano di investimenti economici** per stimolare la ripresa socioeconomica a lungo termine nel vicinato meridionale. La nuova Agenda per il Mediterraneo si incentra su **5 settori d'intervento**: **Stato di diritto e sviluppo umano, resilienza, prosperità e transizione digitale; pace e sicurezza; migrazione e mobilità; transizione verde, resilienza climatica, energia e ambiente**. Per l'attuazione dell'Agenda per il Mediterraneo si prevede **uno stanziamento fino a 7 miliardi di euro**, nell'ambito del nuovo strumento di vicinato, cooperazione allo sviluppo e cooperazione internazionale dell'UE, per il periodo 2021-2027.

- rafforzare la **sicurezza dell'UE**, in particolare promuovendo la costruzione di uno **spazio Schengen più forte e più solido**, preparato per le sfide future e sul suo pieno funzionamento. Al fine di gestire efficacemente le pressioni migratorie, la Slovenia si adopererà per compiere **progressi nei negoziati sul Nuovo patto su migrazione e asilo** e **rafforzare il ruolo dell'Unione europea nella dimensione esterna della migrazione**.

  Nel programma si sottolinea l'importanza del regime di Schengen senza controlli alle frontiere e l'**impossibilità** di **implementarlo** negli ultimi anni a causa della **migrazione illegale** e della **pandemia** del COVID 19. La Presidenza slovena si pone come obiettivo prioritario quello di garantire un'attuazione efficace della normativa Schengen, sottolineando la necessità di un approccio più efficace alla gestione dell'**immigrazione clandestina**, di una migliore protezione delle **frontiere esterne** dell'UE, di un sistema di **asilo** funzionante, di una politica più coerente in materia di **rimpatrio**, nonché di una stretta

cooperazione con i Paesi di origine e di transito in materia di migrazione. Il programma richiama altresì i **negoziati** relativi al Patto sulla migrazione e l'asilo, e la ricerca di un consenso politico volto a realizzare i principi di **responsabilità** e **solidarietà**. Secondo il programma, sarà compito della Slovenia garantire un approccio orizzontale e globale nel discutere e adottare le misure e le politiche in tutte le formazioni del Consiglio, dedicando altresì speciale attenzione alla soluzione del problema delle rotte migratorie illegali verso l'UE;

Con una comunicazione del 2 giugno 2021 la Commissione europea ha recentemente fatto il punto sul funzionamento dello spazio Schengen, proponendo una serie di iniziative concernenti i pilastri fondamentali dell'area di libera circolazione: gestione delle **frontiere esterne**; **misure compensative** dell'assenza di controlli alle frontiere interne; ***governance***, comprensiva di un meccanismo di valutazione e monitoraggio.

Si ricordano, inoltre, le proposte normative riconducibili al **Nuovo Patto sulla migrazione e l'asilo**, presentate nel settembre del 2020 e tuttora all'esame dei colegislatori europei. Le misure legislative riguardano, tra l'altro: i **controlli** alle frontiere esterne dei cittadini stranieri che non rispettano i requisiti per l'ingresso nell'UE, comprese le persone salvate in una **operazione SAR** (ricerca e soccorso, *search and rescue*) nelle acque europee; le procedure di asilo; una revisione parziale delle norme previste dal cosiddetto regolamento di **Dublino**; meccanismi di **solidarietà** da parte degli Stati dell'UE nei confronti dei Paesi membri più esposti ai flussi, compresa una disciplina per la gestione di **situazioni di crisi** e di **forza maggiore** causate da pressioni migratorie ingenti. L'iter legislativo di alcune delle proposte presso il Consiglio dell'UE appare particolarmente **complesso**, trattandosi della sede in cui emergono le divergenze relative ai differenti interessi in campo rappresentati dagli Stati membri in funzione della rispettiva e specifica **collocazione geografica**: si tratta in particolare del regime complessivo sui **controlli** alla frontiera e sulle **procedure** di asilo, nonché dei meccanismi di solidarietà che possono essere attivati nei confronti degli Stati membri più esposti ai flussi. Al riguardo, i Paesi cosiddetti **Med - 5** (Italia, Spagna, Grecia, Malta e Cipro) hanno sin dalle prime battute contestato lo sbilanciamento che potrebbero determinare le nuove procedure e che si può riassumere nei seguenti termini: a fronte di un meccanismo che aumenta gli **oneri procedurali** e di **detenzione** nei Paesi di primo ingresso, non si riscontrerebbe un meccanismo di **solidarietà** altrettanto **certo** e **obbligatorio**. Il Governo italiano ha altresì ribadito più volte la necessità di considerare le misure contenute nel Nuovo Patto europeo sulla migrazione e l'asilo secondo una **logica di pacchetto**, cioè basato su un giudizio onnicomprensivo e interconnesso delle singole proposte normative che lo contengono, nell'ottica di realizzare un bilanciamento equilibrato tra principio di **responsabilità** e di **solidarietà**.

Le iniziative normative presentate nell'ambito del Patto sono tuttora all'esame della I Commissione (Affari costituzionali) della Camera dei deputati nell'ambito del dialogo politico.

Il 19 gennaio 2021 la 14a Commissione (Politiche dell'Unione europea) del Senato della Repubblica si è espressa sulle proposte relative al nuovo patto sulla migrazione e l'asilo con la risoluzione Doc. XVIII-*bis* n. 6.

- rafforzare la **cooperazione dell'UE nel campo della sicurezza e della difesa**, e nel **contrasto delle minacce informatiche e ibride**. In tale contesto, l'UE si dovrebbe dotare di misure nell'ambito della politica estera e di sicurezza comune volte a identificare e combattere le minacce ibride in modo più efficace. Occorre, inoltre, collaborare meglio a livello di UE nell'**affrontare le notizie false e la disinformazione** che proviene da paesi terzi, con una **strategia di comunicazione** adeguata. La Presidenza slovena intende inoltre **far avanzare i lavori per la Bussola strategica dell'UE** (*EU Strategic Compass*) e rafforzare le **relazioni tra UE e NATO** per quanto riguarda la **mobilità militare, la cybersicurezza, il contrasto alle minacce ibride**.

  Il Consiglio dell'UE nelle conclusioni del 17 giugno 2020 ha invitato **l'Alto Rappresentante** a **presentare**, in stretta cooperazione con gli Stati membri e basandosi sui contributi di questi ultimi, **entro la fine del 2020**, un'analisi esauriente a 360 gradi di tutte le minacce e le sfide, che fornisca il contesto per l'elaborazione, da parte degli Stati membri, di un **documento** sullo ***Strategic Compass*** che il **Consiglio dovrebbe adottare nel 2022**. L'obiettivo dello *Strategic Compass* è di sviluppare una "**cultura strategica condivisa**", partendo da una visione comune delle minacce che incombono sull'Europa e dei possibili strumenti per farvi fronte e definendo **obiettivi chiari e misurabili in un orizzonte temporale di 5/10 anni** nell'ambito della **sicurezza e difesa.** Lo *Strategic Compass* dovrebbe essere **articolato in due part**i: nella prima parte dovrebbero essere individuate da un lato le **minacce e le sfide** che l'UE ha di fronte, e dall'altro le **risposte** che essa intende mettere in campo; la seconda parte dovrebbe invece essere divisa in quattro aree: a) **gestione delle crisi**: b) **resilienza e vulnerabilità**; c) **sviluppo delle capacità**; d) **partenariati** con paesi e/organizzazioni terze.

Si segnala, inoltre, che per quanto riguarda la **sicurezza interna** il Programma della presidenza slovena prevede tra l'altro, la promozione di una migliore cooperazione e uno scambio di informazioni di polizia nella lotta alla **tratta di esseri umani** e in altre forme di **criminalità transfrontaliera**. Particolare attenzione è prestata altresì alla lotta al **terrorismo** e alle varie forme di **radicalizzazione** religiosa o ideologica, tema rispetto al quale la Presidenza slovena ritiene di rafforzare la cooperazione dell'UE con l'Islam

umanista e i Paesi che lo praticano. Da ultimo si ricorda che nel settore degli affari interni la Presidenza slovena intende, tra l'altro, adoperarsi per rafforzare la sicurezza interna nell'ambito del sopracitato progetto di riforma della direttiva sulla resilienza delle infrastrutture critiche, nonché per rafforzare il meccanismo di protezione civile dell'UE.

Riunioni interparlamentari nel corso della Presidenza Slovena

Nell'ambito della Presidenza slovena sono previste le seguenti riunioni interparlamentari organizzate dal Parlamento sloveno:

- Riunione dei **Presidenti** della **Conferenza** degli organi parlamentari specializzati negli affari dell'Unione dei parlamenti dell'Unione europea (**COSAC**) - Videoconferenza 19 luglio 2021;
- **Conferenza** interparlamentare sulla politica estera e di sicurezza comune (**PESC**) e sulla politica di sicurezza e difesa comune (**PSDC**), formato da confermare, 8-9 settembre 2021;
- **Conferenza** sul **Semestre europeo** e **Conferenza** interparlamentare sulla stabilità, il coordinamento e la ***governance*** nell'Unione europea - Videoconferenza, 28 settembre 2021;
- Nona riunione del **Gruppo di controllo parlamentare congiunto su Europol** (**JPSG**) – Bruxelles, 25-26 ottobre 2021;
- **Conferenza interparlamentare** di alto livello sulla **migrazione** e l'**asilo** in Europa – Bruxelles, novembre 2021;
- **LXVI Conferenza** degli organi parlamentari specializzati negli affari dell'Unione dei parlamenti dell'Unione europea (**COSAC**) - Formato da confermare, 28-30 novembre 2021;
- Riunione della Commissione per le libertà civili, la giustizia e gli affari interni (**LIBE**) del Parlamento europeo sulla valutazione delle attività di **Eurojust**, Bruxelles, novembre – dicembre 2021;
- Riunione dei **Segretari generali dei Parlamenti dell'UE** – Lubiana, 30-31 gennaio 2022;
- **Conferenza dei Presidenti dei Parlamenti dell'UE** - Lubiana, 4-5 aprile 2022.

II SESSIONE - LA CIBERSICUREZZA NELL'UNIONE EUROPEA: RAFFORZARE LA RESILIENZA DELLE INFRASTRUTTURE CRITICHE E LA CIBERDIFESA

Con l'accelerazione della digitalizzazione, la sicurezza informatica è divenuta una delle componenti più importanti della sicurezza globale. Gli attacchi informatici e la criminalità informatica stanno aumentando in tutta Europa in termini sia di quantità che di sofisticazione; una tendenza destinata a crescere in futuro, visto che il numero dei dispositivi connessi, fra cui macchine, sensori, componenti industriali e reti che costituiscono l'internet degli oggetti (IoT), continua a crescere.

Si prevede che, entro il 2024, in tutto il mondo i dispositivi collegati all'IoT saranno 22,3 miliardi[1]. Inoltre, in base a stime dell'associazione internazionale dei gestori di telefonia mobile (Gsma)[2] i dispositivi connessi superano già il numero delle persone sul pianeta, e il loro numero dovrebbe salire a 25 miliardi entro il 2025, di cui un quarto si troverà in Europa. La pandemia di Covid-19 ha d'altra parte accelerato la digitalizzazione dei modelli di lavoro. Tutto questo ha accresciuto le vulnerabilità agli attacchi informatici, come segnalato in *"The Internet Organised Crime Threat Assessment"* (IOCTA), la relazione pubblicata ogni anno dal Centro europeo per la lotta alla criminalità informatica (EC3) al fine di illustrare i principali risultati, le minacce emergenti e gli sviluppi in merito al *cybercrime*.

Nella comunicazione dal titolo "La strategia dell'Ue in materia di cibersicurezza per il decennio digitale", la Commissione europea afferma che la cibersicurezza è fondamentale per creare un'Europa digitale, verde e resiliente.

L'Unione europea intende rispondere alle sfide **in materia di cibersicurezza** attraverso una serie di meccanismi e misure, che coinvolgono i seguenti sei settori chiave:

1) accrescere la ciberresilienza;

2) proteggere le infrastrutture critiche;

3) combattere la criminalità informatica;

4) rafforzare la diplomazia informatica;

---

[1] Come segnalato nella risoluzione del Parlamento europeo, del 10 giugno 2021, sulla strategia dell'Ue in materia di cibersicurezza per il decennio digitale.

[2] L'International Data Corporation (IDC) prevede 42,6 miliardi di macchine, sensori e telecamere connessi.

5) intensificare la ciberdifesa;

6) promuovere la ricerca e l'innovazione nella sicurezza informatica.

La strategia dell'Ue in materia di cibersicurezza per il decennio digitale

Il 16 dicembre 2020 la Commissione europea e l'Alto rappresentante per gli affari esteri hanno presentato la comunicazione congiunta al Parlamento europeo e al Consiglio dal titolo "La strategia dell'Ue in materia di cibersicurezza per il decennio digitale".

Come evidenziato nella comunicazione, la strategia rappresenta una "componente chiave" del documento "Plasmare il futuro digitale dell'Europa" (COM(2020)67), del piano per la ripresa europea della Commissione ("Il momento dell'Europa: riparare i danni e preparare il futuro per la prossima generazione" - COM(2020)456), della strategia dell'Ue per l'Unione della sicurezza 2020-2025 (COM(2020)605), della strategia globale per la politica estera e di sicurezza dell'Unione europea e dell'agenda strategica del Consiglio europeo 2019-2024.

La strategia definisce in che modo l'Ue intende proteggere i cittadini, le imprese e le istituzioni dalle minacce informatiche, promuovere la cooperazione internazionale e contribuire a garantire un'Internet globale e aperta. A tal fine, facendo seguito ai progressi conseguiti con le strategie precedenti, la comunicazione delinea proposte concrete per l'attuazione di tre strumenti principali - normativi, di investimento e politici - per tre settori di intervento dell'Ue:

1) **resilienza, sovranità tecnologica e *leadership***.

   La strategia evidenzia che tutti gli elementi connessi a Internet nell'Ue (automobili automatizzate, sistemi di controllo industriale o elettrodomestici, l'intera catena di approvvigionamento) devono essere sicuri fin dalla progettazione, resilienti agli incidenti informatici e, nel caso vengano scoperte vulnerabilità, queste devono poter essere corrette rapidamente. Tali aspetti sono ritenuti fondamentali per dare al settore pubblico e privato dell'Ue la possibilità di scegliere **infrastrutture resilienti** e **servizi critici più sicuri**.

   Viene proposto di riformare le norme Ue in materia di sicurezza delle reti e dei sistemi informativi (NIS) nell'ambito di una direttiva NIS riveduta (cfr. la proposta di direttiva relativa a misure per un livello comune

elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148[3] - COM(2020)823) al fine di accrescere il livello di ciberresilienza di tutti i settori pertinenti, pubblici e privati, che svolgono una funzione importante per l'economia e la società. La riforma della direttiva NIS dovrebbe fornire le basi per norme più specifiche, necessarie anche per i settori strategicamente importanti, compresi quelli dell'energia, dei trasporti e della sanità.

Nella strategia viene inoltre proposto di creare una rete di centri operativi per la sicurezza all'interno dell'Ue - un "**ciberscudo europeo**" - al fine di sostenere il miglioramento dei centri esistenti e di istituirne di nuovi. I centri dovrebbero essere in grado di condividere e correlare in modo più efficiente i segnali rilevati, nonché di creare una *intelligence* di alta qualità sulle minacce da condividere con i **centri di condivisione e di analisi delle informazioni** (gli Isac) e le autorità nazionali, consentendo in tal modo una maggiore consapevolezza situazionale. L'obiettivo sarebbe quello di collegare, per fasi, il maggior numero possibile di centri in tutta l'Unione al fine di sviluppare una conoscenza collettiva e condividere le migliori pratiche.

Si sottolinea, fra l'altro, l'importanza di sostenere la formazione e lo sviluppo di competenze dei lavoratori impegnati in tali centri e, sulla base di un'analisi delle esigenze effettuata presso i portatori di interessi e con il contributo dell'Agenzia dell'Unione europea per la cibersicurezza (Enisa), potrebbero essere stanziati oltre 300 milioni di euro a sostegno della cooperazione pubblico-privata e transfrontaliera al fine di creare reti nazionali e settoriali che coinvolgano anche le PMI e si basino su adeguate disposizioni in materia di *governance*, condivisione dei dati e sicurezza.

Si ritiene componente importante della protezione contro le minacce informatiche in generale gli sforzi dell'Ue per migliorare le **competenze informatiche** della forza lavoro, attrarre e trattenere i migliori talenti in materia di cibersicurezza e gli investimenti nella ricerca e nell'innovazione a livello mondiale;

---

[3] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

2) **sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta**;

Attraverso la piena attuazione degli strumenti normativi, la mobilitazione[4] e la cooperazione, l'Ue mira a sostenere gli Stati membri nella difesa dei loro cittadini, nonché dei loro interessi economici e di sicurezza nazionale, nel pieno rispetto dei diritti e delle libertà fondamentali e dello Stato di diritto.

La strategia propone la creazione di un'**unità congiunta per il ciberspazio** che avrebbe la funzione di piattaforma virtuale e fisica per la cooperazione fra le varie comunità di cibersicurezza all'interno dell'Ue, con particolare attenzione al coordinamento tecnico e operativo volto a contrastare gravi minacce e incidenti informatici di natura transfrontaliera.

L'Unità congiunta dovrebbe colmare due grandi lacune che si ritiene attualmente aumentino le vulnerabilità e creino inefficienze nella risposta alle minacce e agli incidenti transfrontalieri che interessano l'Unione: 1) le comunità civili, diplomatiche, delle forze dell'ordine e della difesa in materia di cibersicurezza non dispongono ancora di uno spazio comune per incoraggiare una cooperazione strutturata e facilitare la cooperazione operativa e tecnica; 2) i portatori di interessi in materia di cibersicurezza non sono ancora in grado di sfruttare appieno il potenziale della cooperazione operativa e dell'assistenza reciproca all'interno delle reti e delle comunità già esistenti.

Inoltre, al fine di garantire la sicurezza informatica, la strategia ritiene necessario: contrastare efficacemente la **criminalità informatica**, promuovendo la cooperazione e lo scambio fra gli attori impegnati nella cibersicurezza e le forze dell'ordine; utilizzare un pacchetto di strumenti della **diplomazia informatica**[5]; promuovere le capacità di **ciberdifesa**,

---

[4] Diverse comunità, formate da reti, istituzioni, organismi e agenzie dell'Ue, nonché autorità degli Stati membri, hanno la responsabilità di prevenire, scoraggiare, dissuadere e rispondere alle minacce informatiche, utilizzando i rispettivi strumenti e iniziative. Tali comunità comprendono: i) autorità NIS, quali i gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), e gli organismi di reazione alle catastrofi; ii) autorità giudiziarie e di contrasto; iii) la diplomazia informatica; iv) la ciberdifesa.

[5] Il 19 giugno 2017 il Consiglio Ue ha adottato conclusioni su un quadro relativo a una risposta diplomatica comune dell'Ue alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica").

coerentemente al livello di ambizione dell'Ue derivante dalla strategia globale per il 2016[6];

3) **promozione di un ciberspazio globale e aperto**.

La strategia evidenzia che l'Ue dovrebbe continuare a collaborare con i partner internazionali per promuovere un modello politico e una visione del ciberspazio fondato sullo Stato di diritto, sui diritti umani, sulle libertà fondamentali e sui valori democratici che generino sviluppo sociale, economico e politico a livello globale e contribuiscano a un'Unione della sicurezza. A tal fine, l'Ue dovrebbe lavorare con i Paesi terzi, le organizzazioni internazionali e la comunità multipartecipativa per sviluppare e attuare una politica internazionale in materia di ciberspazio coerente e olistica che tenga conto della crescente interconnessione fra gli aspetti economici delle nuove tecnologie, la sicurezza interna e le politiche estere, di sicurezza e di difesa.

L'Ue dovrebbe inoltre: intensificare il suo impegno e la sua *leadership* nei **processi di normazione internazionale**[7], nonché rafforzare la propria rappresentanza negli organismi di normazione internazionali ed europei e in altre organizzazioni per lo sviluppo di norme; promuovere la sicurezza e la stabilità internazionali nel ciberspazio, in particolare attraverso la proposta dell'Ue e dei suoi Stati membri di un programma d'azione per promuovere un comportamento responsabile degli Stati nel ciberspazio (PoA) in seno alle **Nazioni Unite**; rafforzare ed espandere i dialoghi in materia di ciberspazio con i Paesi terzi per promuovere i suoi

---

[6] Vd. le conclusioni del Consiglio, del 14 novembre 2016, sull'attuazione della strategia globale dell'Ue nel settore della sicurezza e della difesa. La strategia sottolinea l'importanza che l'Alto rappresentante, in collaborazione con la Commissione, presenti una revisione del quadro strategico in materia di ciberdifesa al fine di migliorare ulteriormente il coordinamento e la cooperazione fra attori dell'Ue, come pure con gli Stati membri e fra di essi, anche per quanto riguarda le missioni e le operazioni della politica di sicurezza e di difesa comune (Psdc). Il quadro strategico in materia di ciberdifesa dovrebbe fornire informazioni per la "bussola strategica" (vd. le conclusioni del Consiglio sulla sicurezza e la difesa del 17 giugno 2020), assicurando che la sicurezza informatica e la ciberdifesa siano ulteriormente integrate nel più ampio programma di sicurezza e difesa.

[7] Ad esempio, International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), International Telecommunication Union (ITU), European Committee for Standardisation (CEN), European Committee for Electrotechnical Standardization (CENELEC), European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF), 3rd Generation Partnership Project (3GPP) e Institute of Electrical and Electronics Engineers (IEEE).

valori e la sua visione del ciberspazio, condividendo le migliori pratiche e cercando di cooperare in modo più efficace, e avviare scambi strutturati con organizzazioni regionali come l'Unione africana, il Forum regionale dell'Associazione delle Nazioni del Sud-est asiatico (Asean), l'Organizzazione degli Stati americani e l'Organizzazione per la sicurezza e la cooperazione in Europa; sulla base delle dichiarazioni congiunte dell'8 luglio 2016 e del 10 luglio 2018, continuare a far progredire la cooperazione Ue-Nato, in particolare per quanto riguarda i requisiti di interoperabilità della ciberdifesa; sviluppare un'agenda dell'Ue per lo sviluppo delle capacità informatiche esterne al fine di orientare gli sforzi in linea con i suoi orientamenti per lo sviluppo delle capacità informatiche esterne e con l'Agenda 2030 per lo sviluppo sostenibile.

Il **22 marzo 2021** il **Consiglio "Affari esteri"** ha adottato conclusioni sulla strategia in materia di cibersicurezza, ribadendo che la cibersicurezza è essenziale per **costruire un'Europa resiliente, verde e digitale**.

I ministri dell'Ue hanno stabilito l'obiettivo fondamentale di raggiungere l'autonomia strategica mantenendo nel contempo un'economia aperta. Particolare rilievo in questo senso è stato dato al rafforzamento della capacità di compiere scelte autonome nel settore della cibersicurezza allo scopo di **potenziare la *leadership* digitale e le capacità strategiche dell'Ue**.

Nelle conclusioni il Consiglio evidenzia una serie di settori d'intervento per i prossimi anni, fra cui:

- i piani relativi alla creazione di una **rete di centri operativi di sicurezza** in tutta l'Ue al fine di monitorare e anticipare i segnali di attacchi alle reti;
- la definizione di un'**unità congiunta per il ciberspazio** che fornisca una chiara focalizzazione del quadro di gestione delle crisi di cibersicurezza dell'Ue;
- il suo fermo impegno ad applicare le misure del **pacchetto di strumenti dell'Ue per il 5G** e completarne rapidamente l'attuazione nonché a proseguire gli sforzi volti a garantire la sicurezza delle reti 5G e lo sviluppo delle future generazioni di reti;
- la necessità di uno sforzo congiunto per accelerare **l'adozione di norme di sicurezza internet chiave**, fondamentali per aumentare il

livello generale di sicurezza e apertura dell'internet globale e rafforzare nel contempo la competitività dell'industria dell'Ue;

- la necessità di sostenere lo sviluppo di una **crittografia forte** quale strumento per proteggere i diritti fondamentali e la sicurezza digitale, garantendo al contempo che le autorità di contrasto e giudiziarie siano in grado di esercitare i loro poteri, sia *online* che *offline*;
- l'aumento dell'efficacia ed efficienza del **pacchetto di strumenti della diplomazia informatica**, prestando particolare attenzione alla prevenzione e al contrasto degli attacchi informatici con effetti sistemici che potrebbero incidere sulle catene di approvvigionamento e infrastrutture critiche e sui servizi essenziali, nonché sulle istituzioni e sui processi democratici e compromettere la sicurezza economica;
- la proposta sull'eventuale istituzione di un **gruppo di lavoro di *intelligence* informatica** al fine di rafforzare la capacità specifica del Centro dell'Ue di analisi dell'*intelligence* situazionale (*Intelligence and situation centre* - IntCen)[8] in questo settore;
- l'importanza di **rafforzare la cooperazione** con le organizzazioni internazionali e i paesi partner al fine di promuovere la comprensione condivisa del panorama delle minacce informatiche;
- la proposta di elaborare un'**agenda dell'Ue per lo sviluppo delle capacità informatiche esterne** al fine di aumentare la ciberresilienza e le capacità a livello mondiale.

Il Consiglio si è impegnato a monitorare i progressi compiuti nell'attuazione delle conclusioni mediante un piano d'azione che sarà periodicamente riesaminato e aggiornato.

Al fine di garantire lo sviluppo, l'attuazione e il monitoraggio delle proposte presentate nella strategia in materia di cibersicurezza, il Consiglio ha sollecitato infine la Commissione e l'Alto rappresentante a definire un piano di attuazione dettagliato.

[8] Il Centro di analisi dell'Unione europea noto come EU INTCEN è uno degli strumenti di cui si avvale il Servizio europeo per l'azione esterna (SEAE) - di cui è parte integrante - e in particolare l'Alto rappresentante dell'Unione.

Proposte normative nel contesto della nuova Strategia dell'Ue per la cibersicurezza

La Commissione europea ha presentato **due proposte normative per contrastare** i rischi attuali e futuri *online* e *offline*: 1) una proposta di direttiva aggiornata per proteggere meglio la rete e i sistemi informativi; 2) una nuova direttiva sulla resilienza delle entità critiche.

1) **Proposta di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (**COM(2020)823)

La proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, di abrogazione della direttiva (UE) 2016/1148, è stata presentata dalla Commissione europea il 16 dicembre 2020.

La proposta si inserisce in un contesto più ampio di strumenti giuridici e di iniziative a livello dell'Unione volte ad aumentare la resilienza dei soggetti pubblici e privati alle minacce nel settore della cibersicurezza. In particolare:

- la direttiva (UE) 2018/1972, che istituisce il codice europeo delle comunicazioni elettroniche;
- la proposta di regolamento relativo alla resilienza operativa digitale per il settore finanziario (COM(2020)595);
- la proposta di direttiva sulla resilienza dei soggetti critici (COM(2020)365);
- la strategia dell'Ue per l'Unione della sicurezza (COM(2020)605).

La Commissione propone l'abrogazione della direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informatici nell'Unione (direttiva NIS) con l'intento di modernizzare il quadro giuridico esistente alla luce della crescente digitalizzazione del mercato interno e della rapida evoluzione delle minacce alla cibersicurezza, fenomeni che si sono ulteriormente amplificati dall'inizio della crisi Covid-19[9].

La valutazione del funzionamento della direttiva NIS, condotta ai fini della valutazione d'impatto (cfr. SWD(2020)344 e SWD(2020)345), ha

[9] Vd. anche gli "Elementi di valutazione sui progetti di atti legislativi dell'Ue" n. 16, a cura del Servizio studi del Senato.

identificato i seguenti problemi: 1) il basso livello di ciberresilienza delle imprese operanti nell'Ue; 2) i diversi livelli di resilienza fra Stati membri e fra settori; 3) il basso livello di "consapevolezza situazionale comune" e la mancanza di una risposta comune alle crisi. La maggioranza delle autorità competenti e delle imprese si è mostrata favorevole a una revisione della direttiva NIS. Secondo le stime fornite dalla Commissione europea, l'opzione strategica prescelta apporterebbe una riduzione, pari a 11,3 miliardi di euro, dei costi degli incidenti di cibersicurezza.

Principali obiettivi del riesame sono:

1. **aumentare il livello di ciberresilienza di un vasto gruppo di imprese operanti nell'Unione europea**;
2. **ridurre le incongruenze in termini di resilienza del mercato interno nei settori già contemplati dalla direttiva vigente** (obiettivo specifico sarà quello di garantire lo stesso regime normativo e un livello comparabile di risorse fra gli Stati membri);
3. **migliorare il livello di consapevolezza situazionale comune e la capacità collettiva di preparazione e risposta** (l'opzione strategica prescelta prevede meccanismi volti a promuovere una maggiore fiducia fra Stati membri incentivando la condivisione di informazioni e garantendo un approccio maggiormente operativo, attraverso la designazione delle autorità nazionali competenti responsabili della gestione di incidenti e crisi su vasta scala).

In base alla direttiva (UE) 2016/1148 gli Stati membri sono responsabili nel determinare quali soggetti soddisfano i criteri per essere considerati operatori di servizi essenziali ("processo di identificazione"). Al fine di eliminare le divergenze fra gli Stati membri a tale riguardo e garantire la certezza del diritto per quanto riguarda gli obblighi di gestione e segnalazione dei rischi per tutti i soggetti pertinenti, la proposta intende stabilire un **criterio uniforme** che determini quali soggetti rientrano nell'ambito di applicazione della direttiva. Tale criterio dovrebbe consistere nell'applicazione della regola della soglia di dimensione, in base alla quale rientrano nell'ambito di applicazione tutte **le medie e le grandi imprese**,

quali definite nella raccomandazione 2003/361/CE della Commissione, che operano nei settori o forniscono il tipo di servizi contemplati[10].

All'art. 1 viene definito l'oggetto della direttiva, la quale, al fine di stabilire misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione:

a) fa obbligo agli Stati membri di adottare **strategie nazionali in materia di cibersicurezza** (artt. da 5 a 11) e designare **autorità nazionali** competenti, punti di contatto unici e *team* di risposta agli incidenti di sicurezza informatica - *computer security incident response team*, CSIRT (artt. da 12 a 16);

b) stabilisce obblighi in materia di gestione e segnalazione dei **rischi di cibersicurezza** per i tipi di soggetti definiti "soggetti essenziali", di cui all'allegato I, e "soggetti importanti", di cui all'allegato II (artt. da 17 a 23);

La proposta della Commissione riguarda i seguenti **settori** e **sottosettori**:

- **soggetti essenziali**: energia (energia elettrica, teleriscaldamento e teleraffrescamento, petrolio, gas e idrogeno), trasporto (aereo, ferroviario, per vie d'acqua e su strada), settore bancario, infrastrutture dei mercati finanziari, settore sanitario, fabbricazione di prodotti farmaceutici e di dispositivi medici critici, acqua potabile, acque reflue, infrastrutture digitali (punti di interscambio Internet, fornitori di servizi DNS, registri dei nomi di dominio di primo livello, fornitori di servizi di *cloud computing*, fornitori di servizi di *data center*, reti per la consegna dei contenuti, prestatori di servizi fiduciari, reti pubbliche di comunicazione elettronica e servizi di comunicazione elettronica), pubblica amministrazione e settore spaziale[11];
- **soggetti importanti**: servizi postali e di corriere, gestione dei rifiuti, sostanze chimiche, settore alimentare, fabbricazione di altri dispositivi medici, computer ed elettronica, macchinari e apparecchiature, veicoli a motore e fornitori di servizi digitali (mercati *online*, motori di ricerca *online* e piattaforme di *social network*).

La Commissione propone altresì di affrontare la questione relativa alla sicurezza delle **catene di approvvigionamento** e delle relazioni fra i fornitori. Il gruppo di

[10] Gli Stati membri godono tuttavia di una certa flessibilità per individuare soggetti più piccoli con un profilo di rischio per la sicurezza elevato.

[11] La proposta elimina la distinzione fra gli operatori di servizi essenziali e i fornitori di servizi digitali; il *considerando* 7) della direttiva sottolinea che tale differenziazione si è rivelata obsoleta, in quanto non riflette l'effettiva importanza dei settori o dei servizi per le attività sociali ed economiche nel mercato interno.

cooperazione - istituito all'art. 12 della direttiva[12] -, in collaborazione con la Commissione e l'Enisa (l'Agenzia dell'Unione europea per la cibersicurezza), può effettuare valutazioni coordinate dei rischi delle catene di approvvigionamento critiche di servizi, sistemi o prodotti delle tecnologie dell'informazione e della comunicazione (TIC), basandosi sull'approccio adottato nel contesto della raccomandazione della Commissione sulla cibersicurezza delle reti 5G.

c) stabilisce obblighi in materia di **condivisione delle informazioni** sulla cibersicurezza (artt. 26 e 27).

Prevede inoltre che alcuni tipi di soggetti - fornitori di servizi DNS[13], registri dei nomi di dominio di primo livello, fornitori di servizi di *cloud computing*, fornitori di servizi di *data center* e fornitori di reti di distribuzione dei contenuti, nonché alcuni fornitori di servizi digitali - siano sottoposti alla giurisdizione dello Stato membro in cui hanno lo stabilimento principale nell'Unione. L'Agenzia dell'Unione europea per la cibersicurezza (Enisa) dovrà creare e mantenere un registro dei soggetti di quest'ultimo tipo (artt. 24 e 25).

Gli artt. da 28 a 34 definiscono infine gli aspetti relativi alla vigilanza e all'imposizione di sanzioni.

2) Proposta di direttiva sulla resilienza dei soggetti critici (COM(2020)829)

La proposta espande l'ambito di applicazione della direttiva in materia di infrastrutture critiche (*European Critical Infrastructure* - ECI)[14], di cui si dispone la sostituzione con un nuovo strumento volto ad aumentare la resilienza dei soggetti critici nei settori considerati come essenziali dalla sopra citata proposta di direttiva NIS 2.

La direttiva ECI, che si applica solo ai **settori dell'energia e dei trasporti**, stabilisce una procedura di individuazione e designazione delle infrastrutture

---

[12] Il gruppo di cooperazione è istituito al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni fra gli Stati membri nell'ambito di applicazione della direttiva. È composto da rappresentanti degli Stati membri, della Commissione e dell'Enisa. Il Servizio europeo per l'azione esterna partecipa alle sue attività in qualità di osservatore.

[13] Il sistema dei nomi di dominio (*domain name system*) di cui all'allegato I, punto 8, della proposta di direttiva.

[14] Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.

critiche europee, il cui danneggiamento o la cui distruzione avrebbe un significativo impatto su almeno due Stati membri; dispone inoltre requisiti specifici di protezione per gli operatori ECI e per le autorità competenti degli Stati membri.

Ad oggi sono state designate 94 ECI, due terzi delle quali sono situate in tre Stati membri dell'Europa centrale e orientale. La Commissione osserva tuttavia che la portata dell'azione dell'Ue sulla resilienza delle infrastrutture critiche si estende al di là di tali misure e include misure settoriali e intersettoriali riguardanti fra l'altro la capacità di reagire ai cambiamenti climatici, la protezione civile, gli investimenti esteri diretti e la cibersicurezza. Inoltre, gli stessi Stati membri hanno adottato misure proprie in questo settore che divergono le une dalle altre. La Commissione ritiene pertanto che il quadro vigente sulla protezione delle infrastrutture critiche non sia sufficiente e che sia necessario cambiare radicalmente l'impostazione attuale passando dalla protezione di strutture specifiche al rafforzamento della resilienza dei soggetti critici che le gestiscono.

La nuova proposta estende l'ambito di applicazione a **dieci settori**: energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio.

L'obiettivo generale è aumentare la resilienza dei "soggetti critici" rispetto a una serie di **rischi naturali** e di **origine umana**, intenzionali o meno, compresi i sinistri, le catastrofi naturali, le emergenze di sanità pubblica come le **pandemie**, e le minacce antagoniste, inclusi i reati di terrorismo.

L'art. 1 definisce l'oggetto e l'ambito di applicazione della direttiva, la quale:

a) fa obbligo agli **Stati membri** di adottare determinate misure volte a **garantire la fornitura nel mercato interno di servizi essenziali** per il mantenimento di funzioni vitali della società o di attività economiche, in particolare di individuare i **soggetti critici** e i soggetti da trattare come equivalenti sotto taluni aspetti e di consentire loro di adempiere ai loro obblighi;

b) stabilisce per i **soggetti critici** obblighi volti a **rafforzare la loro resilienza** e a migliorare la loro capacità di fornire tali servizi nel mercato interno;

c) stabilisce regole riguardanti la **vigilanza sui soggetti critici** e l'esecuzione delle norme da parte di questi, e la specifica sorveglianza dei soggetti critici considerati di particolare rilevanza a livello europeo.

In particolare, l'art. 3 stabilisce che gli Stati membri devono adottare una **strategia per rafforzare la resilienza dei soggetti critici**.

L'articolo 4 dispone che le autorità competenti stilino un elenco di servizi essenziali ed effettuino periodicamente una **valutazione di tutti i rischi** rilevanti che possono ripercuotersi sulla fornitura di tali servizi, allo scopo di individuare i soggetti critici.

Ogni Stato membro dovrà inoltre designare una o più **"autorità competenti"** responsabili della corretta applicazione e, se necessario, dell'esecuzione delle norme della direttiva a livello nazionale; nonché, all'interno dell'autorità competente, un "**punto di contatto unico"** che eserciti una funzione di collegamento per garantire la cooperazione transfrontaliera con le autorità competenti di altri Stati membri e con il gruppo per la resilienza dei soggetti critici di cui all'art. 16.

L'art. 10 prevede che gli Stati membri provvedano affinché i soggetti critici, entro sei mesi dal ricevimento della notifica relativa alla loro individuazione come tali, e successivamente quando necessario e almeno ogni quattro anni **valutino**, basandosi sulle valutazioni dei rischi degli Stati membri e su altre fonti di informazioni pertinenti, **tutti i rischi** rilevanti che possono perturbare le loro operazioni.

Gli Stati membri provvederanno quindi, ai sensi dell'art. 11, affinché i soggetti critici adottino **misure tecniche e organizzative adeguate e proporzionate per garantire la propria resilienza**, incluse le misure necessarie per:

- evitare il verificarsi di incidenti, anche tramite misure di riduzione del rischio di catastrofi e di adattamento ai cambiamenti climatici;
- assicurare un'adeguata protezione fisica di aree, impianti e altre infrastrutture sensibili mediante, fra l'altro, recinzioni, barriere, strumenti e routine di controllo del perimetro nonché attrezzature di rilevamento e controlli dell'accesso;
- resistere alle conseguenze degli incidenti e mitigarle, anche mettendo in atto procedure e protocolli di gestione dei rischi e delle crisi e pratiche di allerta;

- riprendersi dagli incidenti, anche tramite misure di continuità operativa e l'individuazione di catene di approvvigionamento alternative;
- assicurare un'adeguata gestione della sicurezza del personale, anche definendo le categorie di dipendenti che svolgono funzioni critiche, introducendo autorizzazioni di accesso alle aree, impianti e altre infrastrutture sensibili così come alle informazioni sensibili;
- sensibilizzare il personale interessato.

I soggetti critici di particolare rilevanza europea saranno oggetto di una **specifica sorveglianza**.

Ai sensi della definizione dell'art. 14, i **soggetti critici di particolare rilevanza europea** sono i soggetti individuati come critici e che forniscono servizi essenziali a o in più di un terzo degli Stati membri, e notificati come tali alla Commissione.

L'art. 15 definisce le disposizioni in materia di specifica sorveglianza applicabili ai soggetti critici di particolare rilevanza europea prevedendo che, su richiesta di uno o più Stati membri o della Commissione, lo Stato membro in cui è situata l'infrastruttura del soggetto critico di particolare rilevanza europea e tale soggetto critico informino, insieme, la Commissione e il gruppo per la resilienza dei soggetti critici dei risultati della valutazione dei rischi effettuata ai sensi dell'art. 10 e delle misure adottate ai sensi dell'art. 11, così come qualsiasi azione di vigilanza o di esecuzione.

La ciberdifesa

L'Ue coopera in materia di difesa nel ciberspazio attraverso le attività dell'**Agenzia europea per la difesa** (Aed), in collaborazione con l'**Agenzia dell'Ue per la cibersicurezza** (Enisa) e l'**Agenzia dell'Ue per la cooperazione nell'attività di contrasto** (Europol**)**.

L'Aed sostiene gli Stati membri nella creazione di una forza militare qualificata nel settore della ciberdifesa e garantisce la disponibilità di tecnologie di ciberdifesa proattive e reattive.

La citata strategia dell'Ue per la cibersicurezza adottata dalla Commissione e dal Seae si pone l'obiettivo di rafforzare:

- il **coordinamento** della ciberdifesa;

- la cooperazione e lo sviluppo di **capacità** in materia di ciberdifesa.

In tal senso, la strategia evidenzia che l'Ue dovrebbe:

1) rivedere il **quadro strategico dell'Ue in materia di ciberdifesa**. Il quadro dovrebbe fornire informazioni per la futura "bussola strategica" assicurando che la sicurezza informatica e la ciberdifesa siano ulteriormente integrate nel più ampio programma di sicurezza e difesa.

   Si evidenzia l'importanza dello sviluppo e utilizzo di tecnologie chiave come l'intelligenza artificiale (IA), la crittografia e il calcolo quantistico.

   In linea con le priorità di sviluppo delle capacità dell'Ue per il 2018[15] e sulla base dei risultati della prima relazione completa di revisione coordinata annuale sulla difesa (Card), approvata dai ministri della Difesa all'interno del comitato direttivo dell'Aed nel novembre 2020, l'Ue dovrebbe promuovere ulteriormente la cooperazione fra gli Stati membri in materia di ricerca, innovazione e sviluppo delle capacità nel campo della ciberdifesa e incoraggiare gli Stati membri a sfruttare appieno il potenziale della cooperazione strutturata permanente (Pesco) e del Fondo europeo per la difesa (Fed)[16];

2) facilitare lo sviluppo di una "**visione e strategia militari dell'Ue sul ciberspazio come dominio operativo**" per le missioni e le operazioni militari della politica di sicurezza e di difesa comune (Psdc).

   Nel 2018 l'Ue ha individuato il ciberspazio come un dominio operativo (vd. il "Quadro strategico dell'Ue in materia di ciberdifesa").

   Il quadro strategico identifica il ciberspazio come "il quinto dominio operativo che si affianca a quello terrestre, marittimo, aereo e spaziale", ed evidenzia che l'efficace attuazione delle missioni e operazioni dell'Ue dipende sempre più da un accesso ininterrotto a un ciberspazio sicuro e richiede pertanto capacità operative informatiche solide e resilienti. Obiettivo del quadro strategico, aggiornato al 2018, è sviluppare ulteriormente la politica di ciberdifesa dell'Ue tenendo conto degli

[15] Nel giugno 2018 gli Stati membri hanno convenuto, in seno al comitato direttivo dell'Aed, di guidare la cooperazione in materia di difesa a livello dell'Ue.

[16] Regolamento (UE) 2021/697 del Parlamento europeo e del Consiglio, del 29 aprile 2021, che istituisce il Fondo europeo per la difesa e abroga il regolamento (UE) 2018/1092.

opportuni sviluppi in altre sedi e settori pertinenti nonché dell'attuazione del quadro dal 2014[17].

Il quadro strategico individua i settori prioritari per la ciberdifesa e chiarisce il ruolo dei vari attori europei, nel rispetto delle responsabilità e delle competenze degli attori dell'Unione e degli Stati membri come pure del quadro istituzionale dell'Ue e della sua autonomia decisionale. Vi si afferma inoltre che, fatte salve l'organizzazione e la legislazione interne degli Stati membri, la cooperazione civile-militare nel ciberdominio può essere presa in considerazione ad esempio ai fini dello scambio di migliori prassi, dei meccanismi per lo scambio di informazioni e di allarme rapido, delle valutazioni dei rischi in materia di risposta in caso d'incidente, delle iniziative di sensibilizzazione nonché delle attività di formazione e delle esercitazioni. La prossima revisione di tale quadro dovrebbe essere presentata entro la metà del 2022 in stretta consultazione con gli Stati membri.

La rete Cert (*computer emergency response team*) militare[18] - istituita dall'Aed - contribuirà ulteriormente ad aumentare in modo significativo la cooperazione fra gli Stati membri;

3) sostenere **sinergie fra l'industria civile, della difesa e dello spazio**.

Il piano d'azione della Commissione sulle sinergie tra l'industria civile, della difesa e dello spazio (COM(2021)71), presentato il 22 febbraio 2021, comprende azioni per sostenere ulteriormente le sinergie a livello di programmi, tecnologie, innovazione e *start-up*, in linea con la *governance* dei rispettivi programmi, quali Orizzonte Europa, Europa digitale e il Fondo europeo per la difesa (Fed).

La strategia sottolinea inoltre che dovrebbero essere sviluppate pertinenti sinergie e interfacce fra le iniziative di ciberdifesa portate avanti in altri contesti, compresi i progetti di collaborazione in materia informatica degli Stati membri nell'ambito della cooperazione strutturata permanente (Pesco), nonché con le strutture di cibersicurezza dell'Ue, per sostenere la condivisione delle informazioni e il sostegno reciproco;

4) rinforzare la **cibersicurezza delle infrastrutture spaziali critiche** nell'ambito del programma spaziale.

---

[17] Il quadro strategico dell'Ue in materia di ciberdifesa è stato adottato dal Consiglio il 18 novembre 2014.

[18] La creazione di una rete Cert militare dell'Ue risponde a un obiettivo identificato nel quadro strategico dell'Ue in materia di ciberdifesa del 2018 e mira a promuovere l'interazione attiva e lo scambio di informazioni fra le Cert militari degli Stati membri dell'Ue.

Per garantire la cibersicurezza delle infrastrutture spaziali critiche sotto la responsabilità del programma spaziale, l'Agenzia europea per il programma spaziale (Euspa) e in particolare il Centro di monitoraggio della sicurezza Galileo saranno rafforzati e il loro mandato sarà esteso ad altre risorse critiche del programma spaziale.

L'Agenzia dell'Ue per la cibersicurezza (Enisa)

L'Enisa, Agenzia dell'Unione europea per la cibersicurezza, è un centro di competenze in materia di sicurezza informatica in Europa, con sede a Heraklion (Grecia).

Istituita nel 2004 con il regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, gli obiettivi, i compiti e gli aspetti organizzativi relativi all'Enisa sono ora stabiliti dal regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, "relativo all'Enisa, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ('regolamento sulla cibersicurezza')".

L'agenzia fornisce consigli pratici e soluzioni per il settore pubblico e privato negli Stati membri e per le istituzioni dell'Ue. Fra le sue attività rientrano:

- l'organizzazione di esercitazioni di crisi informatiche in tutta Europa;
- l'assistenza per lo sviluppo di strategie nazionali di sicurezza informatica;
- la promozione della cooperazione fra le squadre di pronto intervento informatico e lo sviluppo di capacità;

L'Enisa pubblica inoltre relazioni e studi su questioni relative alla sicurezza informatica, fra cui: sicurezza del cloud, protezione dei dati, tecnologie per migliorare la tutela della vita privata e tutela della privacy con le nuove tecnologie, identificazione elettronica e servizi fiduciari elettronici, individuazione delle minacce informatiche.

Maggiori informazioni sul lavoro dell'Enisa sono disponibili nel programma annuale di lavoro dell'agenzia.

Gli organi dell'agenzia comprendono un direttore esecutivo (carica attualmente ricoperta da Juhan Lepassaar), un consiglio di

amministrazioneen, un comitato esecutivo e un gruppo permanente di parti interessate.

L'agenzia lavora in stretta collaborazione con Europol e il Centro europeo per la lotta alla criminalità informatica (EC3).

Inoltre, ha assistito le seguenti agenzie dell'Ue su questioni di sicurezza informatica:

- l'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (Cepol);
- l'Organismo dei regolatori europei delle comunicazioni elettroniche (Berec);
- l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia (eu-LISA);
- l'Agenzia europea per la sicurezza aerea (Aesa).

***

Per approfondimenti sulla **normativa italiana** in materia di cibersicurezza, si rimanda al **Dossier** n. 403 "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale. D.L. 82/2021 - A.C. 3161", del 22 giugno 2021, a cura del Servizio Studi del Senato della Repubblica e del Servizio Studi e dell'Ufficio per i rapporti con l'Unione europea della Camera dei deputati.