

XIV COMMISSIONE PERMANENTE

(Politiche dell'Unione europea)

S O M M A R I O

SEDE CONSULTIVA:

DL 82/2021: Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale. C. 3161 Governo (Parere alle Commissioni I e IX) (<i>Esame e rinvio</i>)	182
---	-----

ATTI DELL'UNIONE EUROPEA:

Proposta di direttiva del Parlamento europeo e del Consiglio volta a rafforzare l'applicazione del principio della parità di retribuzione tra uomini e donne per uno stesso lavoro o per un lavoro di pari valore attraverso la trasparenza delle retribuzioni e meccanismi esecutivi. COM(2021)93 final (Parere alla XI Commissione) (<i>Seguito dell'esame e conclusione – Parere favorevole con osservazioni</i>)	186
ALLEGATO (<i>Parere approvato dalla Commissione</i>)	187
AVVERTENZA	186

SEDE CONSULTIVA

Mercoledì 7 luglio 2021. — Presidenza della vicepresidente Emanuela ROSSINI.

La seduta comincia alle 14.

DL 82/2021: Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

C. 3161 Governo.

(Parere alle Commissioni I e IX).

(*Esame e rinvio*).

La Commissione inizia l'esame del provvedimento in titolo.

Alessandro GIGLIO VIGNA (LEGA), *relatore*, ricorda che la Commissione è chiamata a esaminare, ai fini del parere da rendere alle Commissioni I, Affari costituzionali, e IX, Trasporti, il disegno di legge di

conversione del decreto-legge 14 giugno 2021, n. 82, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

In via preliminare osserva che, in considerazione dell'accresciuta esposizione a minacce cibernetiche, è emersa negli anni la necessità di sviluppare rapidamente meccanismi di tutela. Tale esigenza è aumentata negli ultimi anni anche alla luce delle misure volte a garantire infrastrutture *cloud* sicure e centri dati con elevati standard di qualità nella direzione di una crescente interoperabilità e condivisione delle informazioni.

Ricorda quindi che a livello di Unione europea, la direttiva (UE) 2016/1148 del 6 luglio 2016 (cosiddetta direttiva NIS – *Network and Information Security*), reca misure volte a conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad

incrementare il livello comune di sicurezza nell'Unione europea. Tale direttiva è stata recepita nell'ordinamento italiano con il decreto legislativo n. 65 del 18 maggio 2018, che detta quindi la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS. Successivamente, è stato adottato il decreto-legge n. 105 del 2019 (cosiddetto decreto-legge perimetro), sempre al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure dirette a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi.

Ricorda, inoltre, che la sicurezza cibernetica costituisce uno degli interventi previsti dal Piano nazionale di ripresa e resilienza (PNRR), nell'ambito della componente 1, « Digitalizzazione, innovazione e sicurezza nella PA », compresa nella Missione 1, « Digitalizzazione, innovazione, competitività, cultura e turismo », cui sono destinati circa 620 milioni di euro, di cui 241 milioni di euro per la creazione di una infrastruttura nazionale per la cybersicurezza; 231 milioni di euro per il rafforzamento delle principali strutture operative del perimetro di sicurezza nazionale cibernetica (PSNC); 150 milioni di euro per il rafforzamento delle capacità nazionali di difesa informatica presso il ministero dell'Interno, Difesa, Guardia di Finanza, Giustizia e Consiglio di Stato.

Nell'ambito di tale cornice, il provvedimento in esame interviene a definire l'architettura nazionale della cybersicurezza, identificando gli organi ad essa preposti, le loro funzioni e dotazioni di personale, nonché i connessi obblighi informativi al Parlamento.

Più in dettaglio, il decreto si compone di 19 articoli, i primi 4 dei quali definiscono il sistema nazionale di sicurezza cibernetica, che ha al suo vertice il Presidente del

Consiglio dei ministri, cui è attribuita l'alta direzione e la responsabilità generale delle « politiche di cybersicurezza », e a cui spetta l'adozione della relativa strategia nazionale e la nomina e la revoca del direttore generale e del vice direttore generale della nuova Agenzia per la cybersicurezza nazionale istituita dall'articolo 5 del provvedimento in esame, previa informativa al presidente del COPASIR (articolo 2).

Il Presidente del Consiglio dei ministri può delegare alla Autorità delegata per il sistema di informazione per la sicurezza della Repubblica, ove istituita, le funzioni che non sono a lui attribuite in via esclusiva (articolo 3). Presso la Presidenza del Consiglio dei ministri viene poi istituito il Comitato interministeriale per la cybersicurezza (CIC), organismo con funzioni di consulenza, proposta e vigilanza in materia di politiche di cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico (articolo 4).

Gli articoli 5, 6, 7, 11 e 12 istituiscono l'Agenzia per la cybersicurezza nazionale a tutela degli interessi nazionali nel settore e della sicurezza nazionale nello spazio cibernetico (articolo 5), ne definiscono la sede – a Roma fatta salva la possibilità di sedi secondarie –, e l'organizzazione (articolo 6), le funzioni (articolo 7), le risorse finanziarie (articolo 11) e la dotazione di personale (articolo 12).

L'istituzione dell'Agenzia è strumentale all'esercizio delle competenze che il decreto-legge assegna al Presidente del Consiglio dei ministri e all'Autorità delegata, ove istituita (articolo 5, comma 2). Per lo svolgimento dei suoi compiti istituzionali, è specificato che l'Agenzia può richiedere, anche sulla base di apposite convenzioni e nel rispetto degli ambiti di rispettiva competenza, la collaborazione di altri organi dello Stato, di altre amministrazioni, delle forze di polizia o di enti pubblici (articolo 5, comma 5). L'Agenzia ha personalità giuridica di diritto pubblico ed è dotata di autonomia regolamentare, amministrativa, patrimoniale, organizzativa, contabile e finanziaria. A tal fine essa adotta appositi regolamenti previo parere del COPASIR,

sentito il nuovo Comitato interministeriale per la cybersicurezza.

Le funzioni dell'Agenzia (articolo 7) riguardano il suo ruolo di Autorità nazionale ai fini del complesso di relazioni e funzioni disegnato dalle norme europee ed interne, incluse quelle di certificazione della cybersicurezza. In tale quadro, l'Agenzia predispone in primo luogo la strategia nazionale di cybersicurezza; assume compiti finora attribuiti a diversi soggetti, quali il Ministero dello sviluppo economico, la Presidenza del Consiglio, il Dipartimento delle informazioni e della sicurezza e l'Agenzia per l'Italia digitale. L'agenzia promuove inoltre iniziative per lo sviluppo di competenze e capacità in ambito cibernetico.

Presso l'Agenzia sono inoltre trasferiti il CSIRT italiano (ora CSIRT Italia) e il Centro di valutazione e certificazione nazionale (CVCN). In proposito, ricorda che il CSIRT (*Computer Security Incident Response Team*), è una struttura istituita dal decreto legislativo 18 maggio 2018, n. 65 (di attuazione della direttiva UE 2016/1148- direttiva NIS) e dal decreto del Presidente del Consiglio dei ministri 8 agosto 2019 (« Disposizioni sull'organizzazione e il funzionamento del CSIRT italiano »). Tra i compiti di tale ente sono inclusi il monitoraggio degli incidenti a livello nazionale; l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; l'intervento in caso di incidente; l'analisi dinamica dei rischi e degli incidenti; la sensibilizzazione situazionale. Tra i compiti del CVCN sono invece incluse le valutazioni inerenti all'acquisizione di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti sensibili rientranti nel perimetro della sicurezza nazionale.

Circa il perimetro di sicurezza nazionale cibernetica, segnala che non rientrano tra le funzioni trasferite all'Agenzia quelle spettanti al Ministero per lo sviluppo economico secondo l'attribuzione resa dall'articolo 3 del decreto del Presidente del Consiglio dei ministri n. 131 del 2021, recante regolamento in materia di perimetro di sicurezza nazionale cibernetica, attuativo del decreto-legge n. 105 del 2019. Quell'ar-

ticolo 3 prevede infatti che al Ministero per lo sviluppo economico spettino l'individuazione dei soggetti rientranti nel perimetro, in materia di energia, telecomunicazioni, servizi digitali.

Gli articoli 8 e 9 istituiscono e disciplinano il funzionamento del Nucleo per la cybersicurezza, costituito presso l'Agenzia, quale supporto del Presidente del Consiglio riguardo alle tematiche della cybersicurezza, per gli aspetti relativi alla prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento. L'articolo 10 disciplina invece le procedure da seguire per la gestione delle crisi che coinvolgono aspetti di cybersicurezza specificando in particolare i compiti posti in capo al predetto Nucleo.

Tra le funzioni del Nucleo sono incluse la formulazione di proposte di iniziative in materia di cybersicurezza; la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica; lo svolgimento esercitazioni interministeriali – o la partecipazione italiana ad esercitazioni internazionali – di simulazione di eventi di natura cibernetica; la definizione di procedure di condivisione delle informazioni ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi; la valutazione delle comunicazioni, ricevute, per il tramite del CSIRT Italia, circa i casi di violazioni o tentativi di violazione della sicurezza o di perdita dell'integrità significativi ai fini del corretto funzionamento delle reti e dei servizi e delle notifiche di incidente (circa la tassonomia degli incidenti e la loro notifica, è intervenuto da ultimo il decreto del Presidente del Consiglio dei ministri n. 81 del 2021 e la relativa notifica al Presidente del Consiglio, anche ai fini della convocazione del Comitato interministeriale per la sicurezza della Repubblica (CISR) per la gestione delle predette situazioni di crisi che non possano essere fronteggiate dalle singole amministrazioni).

Per quanto riguarda la disciplina del personale (articolo 12), essa è stabilita in apposito regolamento adottato nel rispetto dei principi generali dell'ordinamento giu-

ridico e dei criteri indicati nel decreto in esame, anche in deroga alle vigenti disposizioni di legge. La deroga è posta in correlazione con le funzioni di tutela della sicurezza nazionale nello spazio cibernetico attribuite all’Agenzia e con le attività svolte dalla medesima in raccordo con il Sistema di informazione per la sicurezza della Repubblica. Il trattamento economico del personale dell’Agenzia è previsto pari a quello in godimento da parte dei dipendenti della Banca d’Italia, in base alla « equiparabilità delle funzioni svolte e del livello di responsabilità rivestito ».

L’articolo 13 prevede che i trattamenti di dati personali per finalità di sicurezza nazionale, in applicazione del decreto-legge in esame, siano effettuati ai sensi del Codice in materia di protezione dei dati personali, con particolare riguardo alle specifiche disposizioni previste per finalità di difesa o di sicurezza dello Stato.

L’articolo 14 prevede la trasmissione al Parlamento di una relazione entro il 30 aprile di ogni anno sull’attività svolta dall’Agenzia nell’anno precedente in materia di cybersicurezza nazionale. Si prevede inoltre che il Presidente del Consiglio dei ministri trasmetta al Comitato parlamentare per la sicurezza della Repubblica (COPASIR) – entro il 30 giugno di ogni anno – una relazione sulle attività svolte nell’anno precedente dall’Agenzia in raccordo con il Sistema di informazione per la sicurezza della Repubblica, nonché in relazione agli ambiti di attività dell’Agenzia sottoposti al controllo del Comitato medesimo ai sensi del decreto-legge in esame.

L’articolo 15 modifica il citato decreto legislativo n. 65 del 2018 (cosiddetto decreto NIS) che ha dato attuazione alla citata direttiva (UE) 2016/1148. Tale decreto legislativo rappresenta la cornice legislativa delle misure per la sicurezza delle reti e dei sistemi informativi e dei soggetti competenti a dare attuazione agli obblighi previsti in tale ambito. Le modifiche recate dall’articolo 15 sono pertanto volte ad adeguare il decreto legislativo n. 65 del 2018 tenendo conto della nuova architettura delineata dal decreto-legge in esame.

L’articolo 16, ai commi da 1 a 7, reca alcune modifiche puntuali alla legislazione vigente anche in tal caso conseguenti al nuovo assetto dell’architettura nazionale di cybersicurezza, al fine di consentire il passaggio delle competenze in materia di perimetro di sicurezza nazionale dal DIS e dal MISE all’Agenzia per la cybersicurezza nazionale, nonché quelle relative, in particolare, al Centro di Valutazione e Certificazione Nazionale (CVCN) e quelle di competenza dell’AgID (commi 1-7). I successivi commi da 8-14 recano innanzi tutto alcune disposizioni di modifica del decreto-legge n. 105 del 2019 volte ad adeguare le disposizioni del citato decreto-legge alle modifiche intervenute (commi 8 e 9), il comma 10 modifica, al fine di integrare con il riferimento ai test effettuati dal CVCN, le disposizioni del decreto-legge n. 21 del 2012 in merito alle comunicazioni da effettuare a cura delle imprese acquirenti impianti per il 5G ai fini dell’esercizio dei poteri speciali, prevedendo inoltre alcune integrazioni e alcune semplificazioni procedurali, il comma 11 inserisce tra le ipotesi di competenza del Tribunale amministrativo regionale del Lazio, sede di Roma, anche le controversie aventi ad oggetto i provvedimenti dell’Agenzia per la cybersicurezza nazionale, i commi 12, 13 e 14 aggiornano al nuovo quadro normativo, con particolare riferimento alle funzioni della citata dell’Agenzia per la cybersicurezza nazionale, le disposizioni della legge di delegazione europea 2019-2020 (comma 12), quelle relative alla definizione della competenza regolamentare in materia di sicurezza e qualità delle infrastrutture digitali per la pubblica amministrazione (comma 13) e del Codice delle Comunicazioni elettroniche (comma 14).

Il particolare, segnala che il citato comma 12 dell’articolo 16 modifica l’articolo 4, comma 1, lettera *b*), della recente legge di delegazione europea 2019-2020 (n.53/2021), che indica i principi ed i criteri direttivi relativi per il recepimento del nuovo codice europeo delle comunicazioni elettroniche, al fine di inserire il riferimento alla nuova Agenzia per la cybersicurezza nazionale tra le autorità competenti per l’attuazione delle

disposizioni del Codice stesso e l'articolo 18 della medesima legge di delegazione, contenente i principi e criteri direttivi per l'adeguamento della normativa nazionale al Regolamento europeo sulla cybersicurezza (Regolamento (UE) 2019/881) al fine di prevedere che ogni riferimento al Ministero dello sviluppo economico, sia da intendersi riferito all'Agenzia per la cybersicurezza nazionale.

L'articolo 17 reca una serie di disposizioni transitorie e finali, mentre l'articolo 18 detta disposizioni relative alla copertura finanziaria relativa alla istituzione dell'Agenzia per la cybersicurezza nazionale per il cui funzionamento è prevista una dotazione crescente, da 2 milioni di euro nel 2021, a 122 milioni a decorrere dal 2027, cui si provvede mediante corrispondente riduzione del Fondo per far fronte ad esigenze indifferibili che si manifestano nel corso della gestione (articolo 1, comma 200, della legge n. 190 del 2014). Osserva pertanto che il finanziamento dell'Agenzia non sembra assorbire le risorse del PNRR ricordate in premessa, finalizzate alla creazione di una infrastruttura nazionale per la cybersicurezza.

L'articolo 19 dispone che il decreto-legge entri in vigore il giorno successivo a quello della sua pubblicazione in *Gazzetta Ufficiale*, ovvero dal 15 giugno 2021.

In conclusione, nel preannunciare il suo orientamento favorevole sul provvedimento in esame, volto a definire un assetto organizzativo strategico in tema di sicurezza nazionale cibernetica, si riserva di formulare una proposta di parere.

Emanuela ROSSINI, *presidente*, nessuno chiedendo di intervenire, rinvia il seguito dell'esame ad altra seduta.

La seduta termina alle 14.10.

ATTI DELL'UNIONE EUROPEA

Mercoledì 7 luglio 2021. — Presidenza della presidente Emanuela ROSSINI.

La seduta comincia alle 14.10.

Proposta di direttiva del Parlamento europeo e del Consiglio volta a rafforzare l'applicazione del principio della parità di retribuzione tra uomini e donne per uno stesso lavoro o per un lavoro di pari valore attraverso la trasparenza delle retribuzioni e meccanismi esecutivi. COM(2021)93 final.

(Parere alla XI Commissione).

(Seguito dell'esame e conclusione – Parere favorevole con osservazioni).

La Commissione prosegue l'esame del provvedimento in titolo, rinviato nella seduta del 27 aprile 2021.

Francesca GALIZIA (M5S), *relatrice*, illustra la proposta di parere favorevole con osservazioni formulata (*vedi allegato*).

La Commissione approva.

La seduta termina alle 14.15.

AVVERTENZA

Il seguente punto all'ordine del giorno non è stato trattato:

SEDE CONSULTIVA

DL 89/2021: Misure urgenti in materia di agricoltura e per il settore ferroviario. C. 3170 Governo.

ALLEGATO

Proposta di direttiva del Parlamento europeo e del Consiglio volta a rafforzare l'applicazione del principio della parità di retribuzione tra uomini e donne per uno stesso lavoro o per un lavoro di pari valore attraverso la trasparenza delle retribuzioni e meccanismi esecutivi (COM(2021)93 final).

PARERE APPROVATO DALLA COMMISSIONE

La XIV Commissione Politiche dell'Unione europea,

esaminata, ai sensi dell'articolo 127, comma 1, del Regolamento, la « Proposta di direttiva del Parlamento europeo e del Consiglio volta a rafforzare l'applicazione del principio della parità di retribuzione tra uomini e donne per uno stesso lavoro o per un lavoro di pari valore attraverso la trasparenza delle retribuzioni e meccanismi esecutivi » (COM(2021)93 final);

premesso che:

l'obbligo di garantire la parità delle retribuzioni è sancito dall'articolo 157 del Trattato sul funzionamento dell'Unione europea (TFUE), che costituisce la base giuridica della proposta di direttiva;

la necessità di garantire la parità salariale è sancita anche nella direttiva 2006/54/CE che, come chiarito dalla Commissione, non è modificata o sostituita dalla nuova iniziativa, dato il suo più ampio ambito di applicazione per combattere la discriminazione basata sul sesso in materia di occupazione e impiego;

la raccomandazione della Commissione 2014/124/UE indirizza agli Stati membri orientamenti che li aiutino a garantire un'applicazione migliore e più efficace del principio della parità retributiva;

l'articolo 23 della Carta dei diritti fondamentali dell'Unione europea stabilisce che la parità tra uomini e donne deve essere assicurata in tutti i campi, anche in materia di occupazione, di lavoro e di retribuzione, e il Pilastro europeo dei diritti sociali include tra i suoi principi la parità di trattamento tra donne e uomini e il diritto alla parità di retribuzione per un lavoro di pari valore;

nonostante il quadro giuridico precedentemente delineato, l'effettiva attuazione del principio della parità salariale tra uomini e donne continua a incontrare una serie di ostacoli, come dimostra il dato sul divario retributivo di genere (*gender pay gap*) nell'Unione europea, che misura la differenza nella retribuzione oraria lorda, in base al quale le donne guadagnano in media il 14,1 per cento in meno all'ora rispetto agli uomini;

il differenziale tra retribuzioni, che si amplifica se si considera il divario retributivo complessivo di genere, determina ripercussioni a lungo termine sulla qualità della vita delle donne, le espone a un maggiore rischio di povertà e perpetua il divario retributivo pensionistico;

considerato che:

i divari di genere nel mondo del lavoro persistono ancora in modo accentuato e la pandemia di COVID-19 ha reso più urgente affrontare questo problema, dato che la crisi ha colpito in modo particolare le lavoratrici;

la proposta di direttiva assume pertanto una rilevanza cruciale e rappresenta una delle più importanti tra quelle preannunciate dalla Commissione europea nella Strategia per la parità di genere 2020-2025 e fa seguito a una valutazione del quadro giuridico dell'Unione europea sulla parità retributiva e a un ciclo di consultazioni pubbliche e indagini mirate, i cui risultati sono riportati nella valutazione d'impatto che accompagna la proposta:

la proposta risponde, altresì, all'invito che il Consiglio dell'UE ha rivolto alla Commissione di elaborare misure concrete per

aumentare la trasparenza retributiva, nonché alla richiesta, avanzata dal Parlamento europeo alla Commissione medesima, di presentare disposizioni vincolanti sulla trasparenza delle retribuzioni e sul divario retributivo tra i generi;

la proposta della Commissione si basa su un'armonizzazione minima dei sistemi degli Stati membri e consente loro, per un verso, di stabilire standard più elevati qualora decidano di farlo e, per l'altro, di affidarne l'attuazione alle parti sociali, a condizione che siano in grado di garantire la realizzazione dei risultati perseguiti dalla direttiva;

rilevato che:

il rispetto del diritto alla parità retributiva tra donne e uomini, sancito dal Trattato, richiede che i datori di lavoro dispongano di strutture retributive volte ad assicurare che le donne e gli uomini ricevano pari retribuzione per lo stesso lavoro o per un lavoro di pari valore;

al fine di consentire ai lavoratori e ai datori di lavoro di valutare ciò che costituisce lavoro di pari valore, la proposta prevede che gli Stati membri stabiliscano strumenti o metodologie per valutare e raffrontare il valore del lavoro, rispetto a una serie di criteri oggettivi che includono i requisiti professionali, di istruzione e di formazione, le competenze, l'impegno e le responsabilità, il lavoro svolto e la natura dei compiti assegnati;

gli articoli 8 e 9 configurano una serie di obblighi concernenti la rendicontazione e la valutazione delle retribuzioni applicabili solo alle aziende con almeno 250 lavoratori, lasciando però agli Stati membri la possibilità di mantenere o stabilire norme più favorevoli per i lavoratori tramite una comunicazione più proattiva di informazioni e di relazioni sulle retribuzioni;

segnalato che il disegno di legge recante deleghe al Governo per il sostegno e la valorizzazione della famiglia, cosiddetta « *Family act* », in corso di esame parlamentare, che rientra tra le riforme di accompagnamento al Piano italiano per la ripresa e la resilienza, contiene misure rilevanti per la

promozione della partecipazione al lavoro delle donne;

considerato inoltre che occorre riconoscere il peso crescente che stanno acquistando le misure di *welfare* aziendale che accompagnano le retribuzioni, attesa l'importanza di tali misure nell'ambito delle politiche di conciliazione dei tempi di vita e di lavoro;

sottolineata, altresì, la necessità che il presente parere, unitamente al documento finale della Commissione di merito, sia trasmesso tempestivamente alla Commissione europea nell'ambito del cosiddetto dialogo politico, nonché al Parlamento europeo e al Consiglio,

esprime

PARERE FAVOREVOLE

con le seguenti osservazioni:

valuti la Commissione di merito l'opportunità di segnalare, nelle competenti sedi europee, che:

a) all'articolo 4, i criteri e le metodologie, volti a valutare e confrontare il valore dei diversi lavori, necessiterebbero di una migliore esplicitazione, prevedendo anche un coinvolgimento delle parti sociali nella relativa definizione;

b) occorrerebbe, altresì, chiarire la previsione, di cui al paragrafo 4 del medesimo articolo 4, che consente un confronto con un lavoratore di riferimento ipotetico, nel caso in cui non sia possibile individuare un lavoratore di riferimento reale, al fine di evitare incertezze interpretative e applicative che ne potrebbero derivare;

c) gli adempimenti di cui agli articoli 8 e 9 dovrebbero essere estesi a una più ampia platea di destinatari, tenuto conto della composizione del tessuto economico e produttivo europeo e della rilevanza delle informazioni sul divario retributivo di genere ai fini del rafforzamento dei meccanismi di trasparenza retributiva.