COMMISSIONE
EUROPEA

Bruxelles, 10.12.2021
COM(2021) 819 final

RELAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Tutela dei diritti fondamentali nell'era digitale -

Relazione annuale 2021 sull'applicazione della Carta dei diritti fondamentali dell'Unione europea

Tutela dei diritti fondamentali nell'era digitale –

Relazione annuale 2021 sull'applicazione della Carta dei diritti fondamentali dell'Unione europea

Indice

1. Introduzione

La Carta dei diritti fondamentali dell'Unione europea[1] è uno strumento efficace utilizzato per proteggere, promuovere e rafforzare i diritti delle persone all'interno dell'Unione europea. I diritti fondamentali non solo proteggono le persone da interferenze indebite come la censura o la sorveglianza di massa, ma consentono anche ai cittadini di esercitare pienamente i loro diritti e sfruttare le loro opportunità nella vita. È sempre possibile migliorare le condizioni e la misura in cui le persone possono godere dei propri diritti. La Carta può orientare le attività politiche in tutta l'UE. Quanto più le persone conoscono i diritti sanciti dalla Carta e sanno come avvalersene, tanto più potere acquisiscono.

La pandemia di COVID-19 ha messo alla prova la tutela e le garanzie dei nostri diritti e delle nostre libertà fondamentali. Qualsiasi limitazione dei diritti fondamentali deve essere necessaria e proporzionata. Lo richiede la Carta dei diritti fondamentali dell'Unione europea, che è giuridicamente vincolante nell'UE. La Carta tutela e promuove un'ampia gamma di diritti connessi alla dignità umana, alla libertà, all'uguaglianza e alla solidarietà, e tutti gli organi giurisdizionali nazionali possono applicarla nei casi in cui il diritto dell'UE viene attuato ed è pertinente ai fini della sentenza definitiva.

Dal 2009 la Carta ha lo stesso status giuridico dei trattati, il diritto primario dell'Unione su cui si basa la legislazione dell'UE. Le istituzioni europee devono rispettarla in tutte le loro azioni e gli Stati membri dell'UE devono conformarvisi quando attuano il diritto dell'Unione.

In quali circostanze gli Stati membri devono conformarsi alla Carta?

- Quando gli Stati membri concordano in sede di Consiglio e con il Parlamento europeo di adottare un nuovo atto normativo dell'UE, è spesso necessario applicare tale atto attraverso misure nazionali di attuazione.

- Quando gli Stati membri adottano o modificano leggi su una materia rispetto alla quale il diritto dell'UE impone obblighi concreti, le loro leggi non possono essere contrarie al diritto dell'UE, compresa la Carta, in quanto tale azione legislativa costituirebbe un'attuazione del diritto dell'UE.

- I programmi di finanziamento dell'UE fanno parte della legislazione dell'UE. Gli Stati membri devono garantire che tali fondi siano spesi secondo le norme previste da tale legislazione. Quando attuano programmi di finanziamento, essi attuano il diritto dell'UE.

- Quando gli Stati membri adottano o modificano leggi in un settore in cui l'UE non ha competenza e per il quale non sono previste leggi dell'UE, essi non attuano il diritto dell'UE. In tali casi, non sono vincolati dalla Carta. Tuttavia molti diritti fondamentali sanciti dalla Carta sono stabiliti contemporaneamente nelle costituzioni e nella giurisprudenza nazionali, nonché nella Convenzione europea dei diritti dell'uomo, di cui tutti gli Stati membri dell'UE sono firmatari.

Per migliorare la conoscenza della Carta da parte di tutti, dal 2010 la Commissione europea pubblica relazioni sulla sua applicazione. Questa edizione è la prima a seguire il nuovo approccio annunciato nella **strategia per rafforzare l'applicazione della Carta dei diritti**

[1] Carta dei diritti fondamentali dell'Unione europea (GU C 326 del 26.10.2012, pag. 391).

fondamentali dell'Unione europea (la strategia di attuazione della Carta)[2]. La relazione annuale si concentrerà su un tema specifico disciplinato dal diritto dell'UE ed esaminerà più da vicino le migliori pratiche e le difficoltà degli Stati membri in tale settore. Ciò consente di esaminare gli sviluppi sistemici per spiegare in che modo i diversi diritti possono rafforzarsi a vicenda e come le evoluzioni politiche, sociali ed economiche possono incidere contemporaneamente su una serie di diritti.

Il tema dell'edizione 2021 è la **tutela dei diritti fondamentali nell'era digitale**, in linea con l'attenzione strategica della Commissione europea nei confronti della transizione digitale.

Su quali informazioni si basa la presente relazione?

La presente relazione è stata elaborata sulla base dei seguenti elementi:

- contributi degli Stati membri dell'UE, i quali sono stati invitati a fornire informazioni sulla base delle rispettive prospettive nazionali[3];

- una consultazione mirata con le organizzazioni ombrello delle organizzazioni della società civile (OSC) europee che operano nel settore dei diritti fondamentali; e

- relazioni delle agenzie dell'UE, in particolare le relazioni annuali sui diritti fondamentali dell'Agenzia dell'Unione europea per i diritti fondamentali (FRA)[4], che contengono una sezione sui diritti fondamentali e la digitalizzazione.

2. Attuare la nuova strategia per rafforzare l'applicazione della Carta dei diritti fondamentali dell'Unione europea

La strategia di attuazione della Carta, adottata dalla Commissione nel 2020, mira a garantire che la Carta sia applicata al massimo delle sue potenzialità, rendendo i diritti fondamentali una realtà per tutti. La strategia di attuazione della Carta definisce il quadro per le attività congiunte in materia di diritti fondamentali in tutta l'UE per i prossimi 10 anni e gode del pieno sostegno degli Stati membri[5]. Le quattro priorità che orientano l'attuazione degli obiettivi definiti nella strategia di attuazione della Carta sono illustrate di seguito.

2.1 Sostenere e monitorare l'effettiva applicazione della Carta negli Stati membri

Le amministrazioni nazionali e locali, i parlamenti e le autorità di contrasto svolgono un ruolo cruciale nel promuovere e tutelare i diritti sanciti dalla Carta e nel creare un contesto favorevole per le organizzazioni della società civile e i difensori dei diritti. La Commissione collabora strettamente con gli Stati membri per aiutarli ad attuare il diritto e le politiche dell'UE in modo efficace e nel pieno rispetto della Carta.

[2] Comunicazione della Commissione "Strategia per rafforzare l'applicazione della Carta dei diritti fondamentali dell'Unione europea", COM(2020) 711.
[3] Gli Stati membri hanno fornito i loro contributi nell'ambito del gruppo di lavoro del Consiglio per i diritti fondamentali, i diritti dei cittadini e la libera circolazione delle persone (FREMP).
[4] https://fra.europa.eu/it/node/41956.
[5] https://data.consilium.europa.eu/doc/document/ST-6795-2021-INIT/it/pdf.

La Commissione sta inoltre aiutando gli Stati membri ad attuare i **programmi finanziati dall'UE** in conformità alla Carta. Il regolamento sulle disposizioni comuni[6] stabilisce le norme che devono essere rispettate nell'utilizzo di diversi fondi dell'UE[7]. Impone agli Stati membri di istituire e utilizzare meccanismi efficaci per garantire la conformità dei programmi finanziati dall'UE alla Carta, come le modalità di rendicontazione al comitato di sorveglianza in merito a casi di denunce riguardanti la Carta o a operazioni sostenute dai fondi non conformi alla Carta. La Commissione continuerà a fornire assistenza tecnica per aiutare gli Stati membri a garantire che i programmi sostenuti dai fondi dell'UE siano elaborati e attuati in modo conforme alla Carta.

Nell'ambito di un regime di finanziamento specifico, il programma Cittadini, uguaglianza, diritti e valori (CERV), la Commissione ha creato nuove **opportunità per le autorità nazionali, regionali e locali** di ricevere finanziamenti per progetti che promuovano una cultura dei valori e rafforzino la conoscenza della Carta[8]. Le città svolgono un ruolo importante nella promozione di tale cultura e nella tutela dei diritti fondamentali. Diverse città hanno aderito a una rete di "città dei diritti umani" e hanno integrato i diritti fondamentali nell'elaborazione delle politiche locali[9]. La FRA ha pubblicato una relazione dal titolo "Diritti umani nell'UE: un quadro per il rafforzamento dei diritti a livello locale" in occasione del suo Forum sui diritti fondamentali tenutosi a ottobre 2021[10]. Il quadro comprende strumenti per aiutare i sindaci, i governi e le amministrazioni locali e le organizzazioni di base a integrare le norme in materia di diritti umani nel loro operato. A seguito del piano d'azione dell'UE contro il razzismo 2020-2025[11], a novembre 2021 la Commissione ha lanciato il "Premio Capitali europee dell'inclusione e della diversità"[12]. Nell'ambito di questa iniziativa saranno assegnati premi per le migliori pratiche in grado di ispirare altre città e regioni europee ai fini della creazione di ambienti più diversificati e inclusivi per i loro abitanti.

Nella strategia di attuazione della Carta la Commissione ha invitato gli Stati membri a designare un **punto di riferimento per la Carta** per agevolare ulteriormente la cooperazione e lo scambio di informazioni sulla sua applicazione. Ad oggi 17 Stati membri hanno designato tale punto di riferimento, che ha un ruolo fondamentale nella diffusione di informazioni e migliori pratiche sulla conoscenza della Carta e nel coordinamento degli sforzi

[6] Regolamento (UE) 2021/1060 del 24 giugno 2021 recante le disposizioni comuni applicabili al Fondo europeo di sviluppo regionale, al Fondo sociale europeo Plus, al Fondo di coesione, al Fondo per una transizione giusta, al Fondo europeo per gli affari marittimi, la pesca e l'acquacoltura, e le regole finanziarie applicabili a tali fondi e al Fondo Asilo, migrazione e integrazione, al Fondo Sicurezza interna e allo Strumento di sostegno finanziario per la gestione delle frontiere e la politica dei visti (GU L 231 del 30.6.2021, pag. 159).

[7] Per il periodo 2021-2027: Fondo europeo di sviluppo regionale, Fondo di coesione, Fondo sociale europeo Plus, Fondo per una transizione giusta, Fondo europeo per gli affari marittimi e la pesca, Fondo Asilo e migrazione, Fondo Sicurezza interna e strumento per la gestione delle frontiere e dei visti.

[8] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/cerv. Nell'ambito dell'invito a presentare proposte per progetti di gemellaggio e reti di città, il programma CERV mette a disposizione 4,2 milioni di EUR nel 2021. Ulteriori informazioni sono disponibili al seguente indirizzo: Funding & tenders (europa.eu).

[9] https://humanrightscities.net/.

[10] https://fra.europa.eu/it/node/42552.

[11] Comunicazione della Commissione "Un'Unione dell'uguaglianza: il piano d'azione dell'UE contro il razzismo 2020-2025", COM(2020) 565 final.

[12] https://eudiversity2022.eu/it/premio/candidare/.

di sviluppo delle capacità nel paese, e contribuisce alla nuova pagina sulle migliori pratiche degli Stati membri per quanto riguarda la Carta, lanciata nel dicembre 2021 sul portale europeo della giustizia elettronica[13].

In qualità di custode dei trattati, la Commissione ha adottato misure concrete per garantire il rispetto dei diritti sanciti dalla Carta nei casi in cui la legislazione o le prassi nazionali di attuazione del diritto dell'UE violino tali diritti, ad esempio avviando procedure di infrazione. In particolare, la Commissione si è adoperata per garantire il rispetto:

- della libertà di associazione delle organizzazioni non governative e del diritto di proteggere i dati personali dei loro donatori;
- della libertà accademica;
- della libertà di espressione e del pluralismo dei media;
- della dignità umana;
- del diritto al rispetto della vita privata;
- del diritto di tutti, comprese le persone LGBTIQ, di non essere discriminati in base al sesso e all'orientamento sessuale.

La Commissione ha monitorato in tutti gli Stati membri le misure di emergenza adottate durante la pandemia di COVID-19 e il loro impatto, in particolare sullo Stato di diritto, sui diritti fondamentali e sul rispetto di altre disposizioni del diritto dell'UE, in linea con la **relazione sullo Stato di diritto 2021** e i capitoli sui singoli paesi[14].

2.2 Responsabilizzare le organizzazioni della società civile, i difensori dei diritti e gli operatori della giustizia

Le organizzazioni della società civile (OSC) e gli organismi nazionali indipendenti per i diritti umani sono partner fondamentali per le istituzioni dell'UE e per gli Stati membri ai fini della promozione e della tutela dei diritti fondamentali, della democrazia e dello Stato di diritto. Sono fondamentali per sensibilizzare i cittadini in merito ai diritti di cui godono e consentire loro di beneficiare di una tutela giurisdizionale effettiva. Tali organizzazioni devono essere in grado di operare in un ambiente favorevole, libero da indebiti vincoli normativi, ostacoli al finanziamento o persino campagne diffamatorie[15], e di sviluppare le proprie capacità. Alcuni Stati membri non dispongono ancora di **istituzioni nazionali per i diritti umani** pienamente funzionanti, che svolgano l'importante ruolo di collegamento tra il governo e la società civile[16]. Gli Stati membri sono invitati a creare tali istituzioni e a garantire che dispongano dei mezzi necessari per operare in piena indipendenza.

[13] https://e-justice.europa.eu/37134/it/member_states_best_practices_on_the_charter.
[14] COM(2021) 700 final, disponibile al seguente indirizzo: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism/2021-rule-law-report_it.
[15] FRA, Proteggere lo spazio civico, 2021, https://fra.europa.eu/it/node/42470.
[16] Cfr. la strategia di attuazione della Carta, op. cit., sezione 2 "Responsabilizzare le organizzazioni della società civile, i difensori dei diritti e gli operatori della giustizia". Cfr. la relazione della FRA dal titolo "Istituzioni nazionali per i diritti umani forti ed efficaci - Sfide, pratiche promettenti e opportunità", disponibile all'indirizzo: https://fra.europa.eu/it/node/40136. I capitoli sui singoli paesi della relazione sullo Stato di diritto 2021 forniscono un resoconto sullo stato di accreditamento delle istituzioni nazionali per i diritti umani: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism/2021-rule-law-report/2021-rule-law-report-communication-and-country-chapters_it.

La Commissione sta **monitorando da vicino la situazione delle OSC** e riferisce in merito agli sviluppi relativi al quadro per la società civile nella sua relazione annuale sullo Stato di diritto. La relazione sullo Stato di diritto 2021 afferma che le OSC hanno risentito della pandemia di COVID-19, non solo a causa dei limiti alla libertà di circolazione e di riunione, ma anche in termini di finanziamento. Secondo la relazione, la partecipazione della società civile all'elaborazione e all'attuazione delle misure relative alla COVID-19 è stata in generale limitata[17]. La relazione sullo Stato di diritto 2020 ha individuato misure che limitano la libertà di espressione delle OSC[18]. I dati raccolti dalla FRA[19] mostrano infatti che molte OSC ritengono che le misure nazionali connesse alla pandemia abbiano avuto un impatto negativo sulle loro attività da marzo 2020. Pur segnalando un aumento della domanda, la maggioranza ha riscontrato difficoltà a continuare a fornire i propri servizi. Tra le sfide pratiche figurano l'annullamento delle attività, l'impatto psicologico sul personale e la riduzione del contributo dei volontari al lavoro.

La Commissione **sostiene inoltre i difensori dei diritti e le OSC** attraverso finanziamenti specifici, come ad esempio un invito a presentare proposte sulla tutela e la promozione dei valori dell'UE, rivolto esclusivamente alle OSC di base e di piccole dimensioni e che erogherà 51 milioni di EUR nel periodo 2021-2022[20]. È stato pubblicato un invito specifico del valore di 2 milioni di EUR per sostenere i contenziosi e lo sviluppo di capacità connessi all'applicazione della Carta[21].

La Commissione sta inoltre promuovendo lo sviluppo di capacità e la **sensibilizzazione dei giudici e degli altri operatori della giustizia in merito alla Carta**. A dicembre 2020 la Commissione ha adottato una nuova strategia europea di formazione giudiziaria per il periodo 2021-2024[22] e a marzo 2021 ha pubblicato un invito a presentare proposte per sostenere progetti di formazione giudiziaria che include i diritti fondamentali tra le sue principali priorità[23]. Sono stati attuati diversi progetti di formazione giudiziaria relativi alla Carta, cofinanziati dalla Commissione nell'ambito del programma Giustizia 2014-2020[24]. Il materiale di formazione giudiziaria sui diritti fondamentali è disponibile per gli operatori della giustizia su una piattaforma lanciata a dicembre 2020[25].

[17] Relazione sullo Stato di diritto 2021, pag. 24.
[18] Relazione sullo Stato di diritto 2020, pag. 16. EUR-Lex - 52020SC0316 - IT - EUR-Lex (europa.eu).
[19] https://fra.europa.eu/it/node/41554; FRA, "Proteggere lo spazio civico", op. cit., cfr. la sezione 1.3. "La COVID-19 aggrava le sfide cui deve far fronte la società civile", pag. 16.
[20] Programma di lavoro del CERV per il periodo 2021-2022.
[21] Invito a presentare proposte per promuovere lo sviluppo di capacità e la sensibilizzazione in merito alla Carta dei diritti fondamentali dell'Unione europea.
[22] COM(2020) 713 final.
[23] Programma Giustizia, Invito a presentare proposte JUST-2021-JTRA, disponibile all'indirizzo: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home.
[24] Ad es. https://era-comm.eu/charter-of-fundamental-rights/seminar-materials/; http://charterclick.ittig.cnr.it:3000/; http://help.elearning.ext.coe.int/.
[25] La piattaforma di formazione europea.

2.3 Utilizzare appieno la Carta dei diritti fondamentali nel processo decisionale dell'UE

Le istituzioni, gli organi e gli organismi dell'Unione devono rispettare la Carta in tutte le loro azioni. La Commissione sta rafforzando le proprie capacità interne in materia di conformità alla Carta e sta aggiornando il pacchetto di strumenti per "Legiferare meglio"[26], compresi gli orientamenti del 2011 per considerazione dei diritti fondamentali nelle valutazioni d'impatto[27]. Sta inoltre elaborando attività di formazione specifiche sulla Carta e uno strumento di e-learning per aiutare il personale a valutare l'impatto delle politiche e delle proposte legislative della Commissione sui diritti fondamentali. Lo strumento di e-learning sarà reso pubblico e potrebbe costituire una risorsa utile, insieme agli orientamenti e al pacchetto di strumenti per "Legiferare meglio" aggiornati, per le altre istituzioni dell'UE e per i legislatori e i responsabili politici negli Stati membri. La Commissione è pronta a sostenere il Parlamento europeo e il Consiglio affinché applichino efficacemente la Carta nel loro operato.

2.4 Rafforzare la consapevolezza dei cittadini

Insieme all'adozione della presente relazione, la Commissione sta avviando una campagna di sensibilizzazione sulla Carta per informare i cittadini in merito ai loro diritti e alle istituzioni cui rivolgersi in caso di violazione degli stessi. La campagna avrà luogo online, attraverso eventi mediatici e i social media, utilizzando l'hashtag **#RightHereRightNow**. Si concentrerà su una serie di diritti specifici, quali la non discriminazione e l'uguaglianza, i diritti del minore, la libertà di espressione e di informazione, il diritto a un ricorso effettivo e a un giudice imparziale. I partner principali, quali le OSC, le istituzioni e gli organismi nazionali per i diritti umani, la FRA e altri organismi e agenzie dell'UE saranno coinvolti nell'attività di sensibilizzazione. Saranno realizzati collegamenti con altre campagne d'informazione sui diritti e con la conferenza sul futuro dell'Europa. La Commissione ha inoltre tradotto la sua pagina web sulla Carta sul sito Europa in tutte le lingue ufficiali dell'UE[28] e ha lanciato una nuova versione del portale europeo della giustizia elettronica, che contiene informazioni sull'applicazione della Carta e sulle istituzioni cui rivolgersi in caso di necessità[29].

3. La Carta come bussola dell'UE per l'era digitale

Per la Commissione europea è prioritario plasmare la transizione digitale in modo che tutti ne traggano vantaggio, nessuno escluso. Quelli che in passato erano descritti come "mondo offline" e "mondo online" oggi stanno diventando indistinguibili. Ciò comporta una serie di difficoltà al fine di garantire il rispetto dei diritti fondamentali in un contesto digitale in rapida evoluzione.

La tecnologia digitale sta permeando sempre di più tutti i settori della nostra società e può essere impiegata in molti modi diversi e spesso vantaggiosi. Le soluzioni digitali

[26] Pacchetto di strumenti per "Legiferare meglio" | Commissione europea (europa.eu).
[27] Orientamenti operativi per tenere conto dei diritti fondamentali nelle valutazioni d'impatto della Commissione europea | Commissione europea (europa.eu).
[28] I tuoi diritti nell'UE | Commissione europea (europa.eu).
[29] https://e-justice.europa.eu/581/IT/fundamental_rights.

promuovono la ricerca scientifica, incrementano la produzione industriale, agevolano la transizione verso la sostenibilità, facilitano una serie di servizi e sono oggi il principale canale di comunicazione pubblica e privata. Offrono inoltre ai cittadini maggiori opportunità per partecipare al dibattito democratico e informarsi su qualsiasi argomento. Nello specifico, i sistemi di intelligenza artificiale possono servire a promuovere l'innovazione e il benessere e possono essere utilizzati dai singoli come strumenti in ogni ambito della vita, ad esempio in quello sanitario, per le attività di traduzione o per supportare il processo decisionale. L'automazione digitale contribuisce a organizzare il lavoro in modo più efficiente e favorisce livelli di coordinamento senza precedenti. La raccolta di dati sulle azioni dell'uomo e sui loro effetti aiuta le persone a comprendere e a plasmare il mondo.

Nel contempo alcuni utilizzi della tecnologia rischiano di limitare l'efficacia della protezione garantita dai diritti fondamentali. La diffusione di contenuti illegali come l'incitamento all'odio e la violenza sessuale su minori mette a rischio il diritto alla dignità della vittima e la diffusione della disinformazione compromette il dibattito democratico e il nostro diritto di accesso all'informazione. Nei casi in cui i processi o persino le decisioni sono automatizzati, può risultare difficile garantire la trasparenza e la responsabilità in relazione ai risultati, ad esempio quando si utilizza un software complesso per decidere in merito alla ripartizione del lavoro. Laddove le informazioni sono carenti o difficili da ottenere, può essere difficile valutare e affrontare le violazioni dei diritti fondamentali.

Quanto più uno strumento automatizzato si basa su fattori esterni quali dati, contributi dei cittadini o altri sistemi per ottenere un risultato, tanto più è difficile garantire che tale strumento non violi i diritti fin dall'inizio, ad esempio a causa di determinati pregiudizi intrinseci che potrebbero influire sul processo decisionale in contesti lavorativi. Quanti più dati sono raccolti sulle persone, tanto più facile è monitorarle e interferire con la loro vita privata. Gli effetti di rete possono ridurre il potere dei singoli nei confronti delle grandi organizzazioni, ad esempio nei mercati online o sulle piattaforme di lavoro, dove le persone hanno scarso potere contrattuale o poche possibilità di organizzarsi. Allo stesso tempo, le piattaforme di social media sono utilizzate anche per diffondere odio e contenuti illegali, ad esempio nei casi di diffusione di forme illecite di incitamento all'odio, materiale pedopornografico o contenuti terroristici. Resta inoltre ancora molto da fare per aiutare tutti a trarre beneficio da strumenti nuovi e utili laddove l'accesso a Internet, le attrezzature o le conoscenze su come utilizzarli sono scarsi.

Tali sfide possono presentarsi singolarmente o in combinazione tra loro, a seconda del contesto. Possono rafforzarsi a vicenda e incidere contemporaneamente su diversi diritti fondamentali: occorre tener conto di questo aspetto per affrontare tali problemi. La presente relazione illustra alcuni degli aspetti chiave che pongono sfide per i diritti fondamentali legate all'uso della tecnologia digitale. Illustra quali diritti sono interessati in questi contesti, come sta evolvendo la situazione negli Stati membri dell'UE e come gli Stati membri e la Commissione europea utilizzano la Carta per superare le diverse difficoltà e tutelare e promuovere i diritti dei cittadini.

4. Affrontare i problemi della moderazione dei contenuti online

Gli intermediari online, come le piattaforme di social media, svolgono un ruolo importante nella vita di ogni cittadino e promuovono nuove forme di interazione tra i singoli individui, le pubbliche amministrazioni e le imprese. Il loro utilizzo ha determinato un aumento significativo delle informazioni disponibili al pubblico e offre ai cittadini maggiori opportunità di esercitare il loro diritto alla libertà di espressione e di accesso alle informazioni, creando anche molteplici spazi per l'attivismo online e l'aggregazione dei singoli individui e della società civile.

Grandi piattaforme, le nuove piazze

- Alcune piattaforme online sono divenute tanto importanti nell'agevolare lo scambio di informazioni da svolgere un ruolo fondamentale nel dibattito democratico.
- Poiché oltre la metà della popolazione dell'UE utilizza i social media, quasi il 90 % nel caso delle persone di età compresa tra i 16 e i 24 anni, gli effetti della progettazione e delle norme su tali piattaforme hanno un impatto sociale di ampia portata[30].
- Gli strumenti e i meccanismi utilizzati da queste piattaforme per moderare i contenuti e incoraggiare le persone a trascorrere il maggior tempo possibile utilizzando il loro servizio svolgono un ruolo fondamentale nel plasmare le informazioni e le opinioni in cui i cittadini si imbattono online.
- Contrastare i contenuti illegali su queste grandi piattaforme risulta difficile poiché esse sono diventate spazi pubblici per lo scambio di informazioni senza essere giuridicamente responsabili di eventuali considerazioni di interesse pubblico.

Nel contempo l'uso delle piattaforme online amplifica problemi sociali quali la polarizzazione[31] o la diffusione di contenuti illegali, spesso con effetti fortemente negativi sui diritti fondamentali quali la tutela dei diritti del minore, la protezione dei consumatori, la libertà di ricevere e comunicare informazioni e la protezione della proprietà intellettuale.

La portata e la velocità della diffusione di contenuti online che non sono di per sé illegali, come la disinformazione e le teorie complottistiche, possono incidere sul dibattito democratico, sulla fiducia nelle istituzioni e, come si è visto in seguito alla pandemia di COVID-19, sulla salute, la sicurezza e la parità di trattamento.

La democrazia nell'UE deve affrontare numerose sfide, tra cui il populismo, un dibattito politico sempre più polarizzato e l'erosione della fiducia dei cittadini nei processi democratici causata dalla disinformazione[32]. Tali fenomeni sono aggravati dall'ingerenza coordinata nelle

[30] https://ec.europa.eu/eurostat/web/products-datasets/-/isoc_sk_dskl_i.

[31] Si vedano gli esempi di rischi sistemici emergenti per la società posti dalle piattaforme online nella valutazione d'impatto allegata alla proposta di regolamento relativo a un mercato unico dei servizi digitali (legge sui servizi digitali), SWD(2020) 348 final, pag. 40 ("Valutazione d'impatto relativa alla legge sui servizi digitali").

[32] Studio del Parlamento europeo richiesto dalla sottocommissione per i diritti dell'uomo, "Impatto della disinformazione sui processi democratici e sui diritti umani nel mondo", Carme Colomina, Héctor Sánchez Margalef, Richard Youngs, disponibile all'indirizzo: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf.

elezioni da parte di paesi terzi o interessi privati, dalla diffusione della disinformazione e dalla mancanza di trasparenza e responsabilità della pubblicità politica mirata. Sono inoltre state espresse preoccupazioni circa il fatto che alcuni gruppi non sono sufficientemente inclusi o coinvolti, come i giovani, gli anziani o le persone con disabilità. Le minoranze etniche, comprese le comunità rom, le persone LGBTIQ e le donne esitano, in varia misura e a seconda del contesto, a impegnarsi a livello politico per timore di intimidazioni, minacce, molestie e incitamento all'odio. In tali circostanze, le misure volte a tutelare i diritti fondamentali contribuiscono direttamente a difendere i valori dell'UE di una società sostenibile, equa, democratica e partecipativa in cui prevalgano la tolleranza, la non discriminazione e il pluralismo.

La libertà di espressione, anche online, è al centro di qualsiasi democrazia. Qualsiasi misura legislativa o non legislativa relativa alla moderazione dei contenuti e alla responsabilità degli intermediari online per i contenuti dei loro servizi deve tenere conto del fatto che il diritto alla libertà di espressione comprende il diritto di esprimere idee che possono essere considerate critiche, offensive, ingiuriose o controverse e che tale diritto può essere limitato solo a determinate condizioni molto rigorose, anche per quanto riguarda la diffusione di contenuti considerati illegali, tra cui materiali di incitamento all'odio. Tuttavia la Corte europea dei diritti dell'uomo ha anche chiarito che gli Stati possono, e in alcuni casi devono, contrastare ogni forma di espressione che diffonda, inciti, promuova o giustifichi l'odio nei confronti di persone o gruppi appartenenti a una particolare etnia o religione[33].

Molto spesso disinformazione e cattiva informazione non sono illegali, sebbene possano risultare inquietanti oppure offensive. Se da un lato l'obbligo primario dello Stato in relazione ai discorsi protetti dalla libertà di espressione è di astenersi da qualsiasi tipo di ingerenza e censura, lo Stato ha anche l'obbligo positivo di garantire un contesto favorevole per un dibattito pubblico pluralistico e inclusivo, in particolare in relazione alle elezioni, e per l'esercizio della libertà dei media. Tali misure vanno al di là della sfera della moderazione dei contenuti e sono collegate ad azioni più sostanziali in materia di istruzione e informazione.

Gli attori privati, quali le piattaforme online, definiscono i relativi termini e modelli operativi nell'esercizio dei propri diritti alla libertà contrattuale e d'impresa in assenza di istruzioni da parte dello Stato in merito al tipo di contenuti che sarebbero tenuti a ospitare. In tale contesto potrebbero adottare misure che incidono in modo significativo sugli utenti e sui loro diritti. Non sempre è disponibile un ricorso legale contro tali decisioni private, che consenta di renderle compatibili con i diritti e gli interessi legittimi degli individui e garantisca un certo livello di prevedibilità. Laddove rimuovano un numero eccessivo di contenuti legali, le piattaforme online possono limitare significativamente la libertà di espressione e di informazione.

4.1 Situazione a livello dei singoli Stati membri

Nel corso della **consultazione mirata** ai fini della presente relazione, gli attori della società civile hanno riferito in merito a problemi negli Stati membri causati da determinati contenuti illegali online, come campagne diffamatorie e attacchi rivolti a coloro che lavorano per proteggere i diritti altrui. È stato riferito che le donne, in particolare le donne di colore o appartenenti a gruppi vulnerabili come migranti e rom, nonché le persone LGBTIQ, sono

[33] Sentenza del 6 luglio 2006, Erbakan/Turchia, § 56.

state colpite in modo sproporzionato. I minori che utilizzano le piattaforme online sono esposti a contenuti inappropriati, dannosi e violenti e a predatori online, il che comporta maggiori rischi di adescamento e reclutamento da parte di ambienti estremisti. È stato segnalato che la violenza sessuale nei confronti dei minori è stata amplificata attraverso Internet, ad esempio a causa dell'aumento della domanda di materiale pedopornografico.

La disinformazione è stata inoltre identificata dalle organizzazioni della società civile come un problema che interessa la salute e la sicurezza, nonché il dibattito democratico in diversi Stati membri. È stata riscontrata una diffusa preoccupazione per la mancanza di trasparenza (etichette, condivisione di segnalazioni, notifiche di esposizione) e di alfabetizzazione mediatica in relazione ai contenuti falsi o fuorvianti.

Se da un lato la diffusione di contenuti illegali e di disinformazione è stata considerata una minaccia, le OSC consultate hanno anche messo in guardia contro gli effetti sulla libertà di espressione dell'utilizzo di politiche di moderazione mal ponderate per far fronte a tali minacce. Le OSC hanno segnalato abusi della protezione del diritto d'autore per mettere a tacere le voci sul web e delle leggi sulla diffamazione e sull'apologia del terrorismo per reprimere comportamenti individuali. La scarsa precisione dei sistemi automatizzati di moderazione dei contenuti, in particolare quando vengono utilizzati su contenuti per i quali la valutazione della legittimità dipende da un elevato livello di contestualizzazione, ha sollevato preoccupazioni in merito agli effetti ingiustificati sulla libertà di espressione dell'eccessiva rimozione dei contenuti e della riduzione al silenzio di determinate dichiarazioni e opinioni, anche espressi da minoranze. Secondo gli accademici e i partecipanti alla consultazione mirata, anche l'uso di algoritmi per personalizzare la visualizzazione dei contenuti per gli utenti può distorcere il dibattito democratico, in quanto è spesso finalizzato ad aumentare gli introiti pubblicitari anziché a fornire ai cittadini informazioni attendibili nel pubblico interesse. Affermazioni analoghe secondo cui gli algoritmi utilizzati per personalizzare i contenuti visualizzati dagli utenti siano dannosi sono state avanzate anche da informatori attraverso la stampa[34]. Al di là degli effetti dell'uso di tali sistemi sui diritti fondamentali, i partecipanti alla consultazione mirata hanno dichiarato che spesso essi sono utilizzati in modo non (del tutto) trasparente e con una scarsa responsabilità in relazione ai loro risultati.

Diversi Stati membri dell'UE hanno regolamentato i servizi digitali disponibili sul loro territorio. Tali leggi mirano a garantire che i prestatori di servizi rispettino determinate norme procedurali quando gli utenti o le autorità segnalano contenuti illegali. Talvolta riguardano categorie specifiche di contenuti illegali, come ad esempio le violazioni del diritto d'autore o forme illecite di incitamento all'odio. Tuttavia i requisiti specifici di tali leggi si discostano spesso gli uni dagli altri per una serie di aspetti, quali:

- le informazioni necessarie per segnalare contenuti illegali;
- la possibilità di reagire a disposizione di coloro che hanno pubblicato tali contenuti;
- il termine entro il quale i prestatori di servizi devono reagire;
- possibili misure obbligatorie contro le segnalazioni infondate; oppure
- la possibilità di sottoporre casi controversi all'attenzione di una terza parte indipendente.

[34] Cfr. ad esempio https://www.theguardian.com/technology/2021/oct/10/frances-haugen-takes-on-facebook-the-making-of-a-modern-us-hero.

Più di recente, a fronte dell'aumento dei timori legati alla diffusione delle forme di incitamento all'odio e dei contenuti terroristici, diversi Stati membri hanno adottato, hanno proposto o prevedono di adottare norme supplementari, concentrandosi in particolare su determinate categorie di contenuti illegali e talvolta anche sui prestatori di servizi stabiliti al di fuori del proprio territorio. Vi è tuttavia una significativa frammentazione giuridica tra le iniziative dei singoli Stati membri per contrastare i contenuti illeciti online e fornire diverse tipologie di salvaguardie per la libertà di espressione. Diversi Stati membri[35], nonché il Consiglio[36] e il Parlamento europeo[37], hanno chiesto che tali preoccupazioni comuni siano affrontate a livello dell'UE. Inoltre vari Stati membri hanno osservato che la mancanza di cooperazione transfrontaliera tra le autorità nazionali ostacola una vigilanza efficace delle piattaforme online che operano a livello transfrontaliero[38].

4.2 La risposta politica dell'UE

Sulla base delle richieste degli Stati membri, sono state adottate diverse iniziative settoriali a livello dell'UE per far fronte al problema di tipi specifici di contenuti illegali come quelli connessi al terrorismo, agli abusi sessuali sui minori, all'incitamento all'odio e alla violenza, alla tratta di esseri umani, ai prodotti non sicuri e alle violazioni del diritto d'autore, assicurando nel contempo la tutela dei diritti fondamentali.

La direttiva sui servizi di media audiovisivi

La **direttiva riveduta sui servizi di media audiovisivi** (AVMS), adottata nel 2018, comprende misure volte a proteggere i minori dai contenuti audiovisivi e dalle comunicazioni commerciali che potrebbero arrecare loro un pregiudizio fisico, mentale o morale. Inoltre, gli Stati membri devono garantire che i servizi di media audiovisivi non contengano istigazioni alla violenza o all'odio nei confronti delle persone fondati sui motivi di cui all'articolo 21 della Carta dei diritti fondamentali dell'Unione europea. Il termine per il recepimento della direttiva era stato fissato al 19 settembre 2020. A novembre 2020 la Commissione ha avviato procedure di infrazione (inviando lettere di costituzione in mora) nei confronti di 23 Stati membri che non avevano recepito la direttiva e molti hanno provveduto al recepimento nel corso dell'anno successivo. A settembre 2021 la Commissione ha inviato un secondo avvertimento (pareri motivati) a nove Stati membri per mancata comunicazione del completo recepimento. L'attuazione della direttiva AVMS riveduta è essenziale non solo per gli operatori del mercato, ma anche per i singoli individui (compresi gli osservatori e i minori).

[35] https://digital-strategy.ec.europa.eu/en/summary-report-open-public-consultation-digital-services-act-package.
[36] Conclusioni del Consiglio del 9 giugno 2020, "Plasmare il futuro digitale dell'Europa" e Conclusioni della riunione straordinaria del Consiglio europeo del 1° e 2 ottobre 2020.
[37] Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione sulla legge sui servizi digitali: migliorare il funzionamento del mercato unico (2020/2018(INL)); risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione sulla legge sui servizi digitali: adeguare le norme di diritto commerciale e civile per i soggetti commerciali che operano online (2020/2019(INL)).
[38] Valutazione d'impatto relativa alla legge sui servizi digitali, sezione 2.3, paragrafo 6, Cooperazione limitata tra gli Stati membri e mancanza di fiducia.

La direttiva sul diritto d'autore nel mercato unico digitale

La **direttiva sul diritto d'autore**[39], adottata ad aprile 2019, mira a garantire che i titolari dei diritti percepiscano un equo compenso per l'utilizzo della loro opera. In questo modo stabilisce un equilibrio tra diritti fondamentali concorrenti quali il diritto alla proprietà intellettuale, la libertà di espressione e di informazione, la libertà scientifica e il diritto all'istruzione e alla diversità culturale. La direttiva introduce eccezioni obbligatorie al diritto d'autore che tutelano la libertà di espressione degli utenti che creano e caricano contenuti sui servizi di condivisione di contenuti online. A norma della direttiva la Commissione deve organizzare un dialogo tra le parti interessate per discutere le migliori prassi per la cooperazione tra i prestatori di servizi di condivisione di contenuti online e i titolari dei diritti, tenendo specialmente conto della necessità di pervenire a un equilibrio tra i diritti fondamentali e il ricorso a eccezioni e limitazioni. A seguito di tale dialogo, a giugno 2021 la Commissione ha adottato orientamenti a sostegno dell'applicazione coerente dell'articolo 17 della direttiva, che stabilisce nuove norme sull'utilizzo di contenuti protetti da parte di prestatori di servizi di condivisione di contenuti online[40]. Gli orientamenti forniscono indicazioni pratiche sulle principali disposizioni dell'articolo 17, aiutando gli operatori del mercato a conformarsi al meglio all'attuazione delle leggi nazionali basate sulla direttiva e tenendo conto delle opinioni raccolte dagli Stati membri e dalle parti interessate.

Il codice di condotta per contrastare l'illecito incitamento all'odio razzista e xenofobo

Nel 2016 la Commissione ha firmato un **codice di condotta** volontario con le principali piattaforme online per garantire che le segnalazioni di casi di **illecito incitamento all'odio razzista e xenofobo** siano verificate in tempi rapidi, non solo alla luce delle condizioni di servizio delle imprese, ma anche delle leggi degli Stati membri utilizzate per attuare il diritto dell'UE che criminalizza l'incitamento all'odio razzista e xenofobo[41]. La conformità al codice di condotta è monitorata periodicamente[42]. Ciò consente di ottenere risultati positivi e ha inoltre favorito un approccio collaborativo tra le piattaforme online, gli Stati membri e la società civile per garantire una moderazione dei contenuti di alta qualità laddove è necessaria una comprensione approfondita del contesto culturale, linguistico e storico dei contenuti controversi.

Raccomandazione sulla sicurezza dei giornalisti e degli altri professionisti dei media

La sicurezza è diventata motivo di grande preoccupazione per i giornalisti, a causa dell'incitamento all'odio online, delle minacce di violenza fisica, ma anche dei rischi connessi alla cibersicurezza e della sorveglianza illegale. Il 16 settembre 2021 la Commissione europea ha pubblicato una **raccomandazione per la protezione, la sicurezza e**

[39] Direttiva 2019/790 (UE) sul diritto d'autore e sui diritti connessi nel mercato unico digitale (GU L 130 del 17.5.2019).
[40] Comunicazione della Commissione, Orientamenti relativi all'articolo 17 della direttiva 2019/790/UE sul diritto d'autore nel mercato unico digitale, COM/2021/288 final.
[41] Decisione quadro 2008/913/GAI, del 28 novembre 2008, sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale (GU L 328 del 6.12.2008).
[42] L'ultimo monitoraggio si è svolto nel 2021: Il codice di condotta dell'UE per contrastare l'illecito incitamento all'odio online | Commissione europea (europa.eu).

l'empowerment dei giornalisti[43]. La raccomandazione invita gli Stati membri a promuovere la cooperazione tra le piattaforme online e le organizzazioni che dispongono di competenze particolari nella lotta contro le minacce nei confronti dei giornalisti, ad esempio incoraggiandone il potenziale ruolo di segnalatori attendibili. I giornalisti e gli altri professionisti dei media non solo sono oggetto di istigazioni all'odio online e minacce di violenza fisica, ma possono anche essere soggetti a sorveglianza illegale; la raccomandazione precisa che gli organismi nazionali competenti in materia di cibersicurezza dovrebbero, su richiesta, assistere i giornalisti che cercano di determinare se i loro dispositivi o account online sono stati compromessi a ottenere i servizi di investigatori forensi in materia di cibersicurezza. Gli Stati membri dovrebbero anche promuovere il dialogo costante tra tali organismi responsabili della cibersicurezza, i media e i rappresentanti del settore, in particolare per promuovere la sensibilizzazione in materia di cibersicurezza e le competenze digitali tra i giornalisti.

Regolamento relativo al contrasto della diffusione di contenuti terroristici online

La sicurezza e il rispetto dei diritti fondamentali non sono obiettivi contrastanti, bensì coerenti e complementari. La sicurezza degli ambienti sia fisici che digitali impone di contrastare i contenuti illegali online. Per garantire la rimozione dei contenuti terroristici, nel 2021 il Parlamento europeo e il Consiglio hanno adottato un **regolamento relativo al contrasto della diffusione di contenuti terroristici online**[44], che contiene una serie di salvaguardie per i diritti fondamentali, in particolare la libertà di espressione. Ad esempio, gli ordini di rimozione da parte delle autorità nazionali possono essere emessi solo per i contenuti terroristici definiti dal regolamento e devono giustificare la motivazione per cui il materiale è considerato contenuto terroristico. Il regolamento esclude i contenuti diffusi per scopi educativi, giornalistici, artistici o di ricerca e a fini di sensibilizzazione contro l'attività terroristica. Per le piattaforme online non vi è alcun obbligo di utilizzare strumenti automatizzati per identificare o rimuovere proattivamente i contenuti terroristici ma, qualora siano utilizzate misure tecniche, dovrebbero essere fornite salvaguardie adeguate, in particolare la sorveglianza e le verifiche umane, per garantire l'accuratezza. A decorrere da marzo 2023, gli Stati membri e le piattaforme online dovranno inoltre pubblicare relazioni annuali sulle misure adottate per rimuovere i contenuti terroristici e sul funzionamento degli strumenti automatizzati eventualmente impiegati.

Legislazione in materia di lotta contro gli abusi sessuali online sui minori

Se l'azione normativa per contrastare i contenuti illegali si è concentrata in larga misura su contenuti accessibili al pubblico come quelli pubblicati sui social media o sui siti web, occorre anche combattere il **materiale pedopornografico** condiviso tramite comunicazioni interpersonali, ivi compresi gli strumenti di comunicazione interpersonale sui social media. Una **normativa provvisoria**[45] entrata in vigore ad agosto 2021 garantisce che determinati

[43] Raccomandazione della Commissione, del 16.9.2021, relativa alla garanzia della protezione, della sicurezza e dell'empowerment dei giornalisti e degli altri professionisti dei media nell'Unione europea, C(2021) 6650 final.
[44] Regolamento 2021/784 relativo al contrasto della diffusione di contenuti terroristici online (GU L 172 del 17.5.2021).
[45] Regolamento 2021/1232 relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE per quanto riguarda l'uso di tecnologie da parte dei fornitori di servizi di comunicazione interpersonale

servizi di comunicazione online, come i servizi di messaggistica o di posta elettronica, possano continuare a utilizzare, nella misura strettamente necessaria, tecnologie specifiche volte a individuare materiale pedopornografico, segnalarlo e rimuoverlo, assicurando nel contempo una serie di garanzie a tutela della vita privata e della protezione dei dati personali ai sensi del regolamento generale sulla protezione dei dati. I meccanismi volti a individuare gli abusi sessuali sui minori nelle comunicazioni interpersonali rischiano di interferire con i diritti fondamentali, in particolare la riservatezza delle comunicazioni, la protezione dei dati personali o la libertà di espressione. Il regolamento provvisorio mira ad attenuare tale effetto limitando l'uso delle tecnologie a quelle meno invasive della vita privata in linea con lo stato dell'arte del settore. Il regolamento prevede inoltre meccanismi di ricorso che devono essere predisposti al fine di garantire che una persona possa presentare un reclamo ai fornitori in caso di rimozione indebita dei propri contenuti. La Commissione sta inoltre preparando una **proposta legislativa** volta a sostituire tale misura provvisoria per garantire ai prestatori di servizi la certezza del diritto e assicurare un approccio uniforme all'individuazione, alla rimozione e alla segnalazione del materiale pedopornografico, garantendo nel contempo il giusto equilibrio tra i diritti del minore e la necessità di proteggere i minori dagli abusi sessuali, nonché il diritto alla vita privata e alle comunicazioni di tutti gli utenti dei servizi online.

Strategia dell'UE per la lotta alla tratta degli esseri umani 2021-2025

Contrastare il modello operativo digitale dei trafficanti è una delle priorità della strategia dell'UE per la lotta alla tratta degli esseri umani 2021-2025[46], presentata dalla Commissione ad aprile 2021. I prestatori di servizi Internet e le imprese collegate fanno parte della soluzione destinata a sostenere gli sforzi anti-tratta tramite l'individuazione e la rimozione di materiale online associato allo sfruttamento e all'abuso di vittime della tratta. La Commissione condurrà un dialogo con le imprese tecnologiche e di Internet pertinenti al fine di ridurre il ricorso a piattaforme online per il reclutamento e lo sfruttamento delle vittime, e favorirà eventuali dialoghi analoghi che saranno condotti dagli Stati membri a livello nazionale.

Proposta di regolamento relativo alla legge sui servizi digitali

La proposta di regolamento relativo alla **legge sui servizi digitali**[47], adottata dalla Commissione nel dicembre 2020 e attualmente all'esame dei colegislatori, definisce le responsabilità degli intermediari online. Fatte salve le norme settoriali dell'UE, come quelle sul diritto d'autore o sui contenuti terroristici online, essa fornisce un unico insieme orizzontale di norme nell'UE per una governance equilibrata della moderazione dei contenuti online.

La proposta garantisce l'adeguata tutela di tutti i diritti fondamentali, compresi la libertà di espressione e il diritto alla vita privata degli utenti, la libertà d'impresa e contrattuale delle

---

indipendenti dal numero per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali online sui minori (GU L 274 del 30.7.2021).

[46] Comunicazione sulla strategia dell'UE per la lotta alla tratta degli esseri umani 2021-2025, COM(2021) 171 final.

[47] Proposta di regolamento relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, COM/2020/825 final.

piattaforme e i relativi diritti di proprietà intellettuale. Mira inoltre a ridurre i rischi per le persone in situazioni di vulnerabilità e i gruppi vulnerabili al fine di proteggerli da minacce, intimidazioni o comportamenti discriminatori e tutelare il diritto alla dignità umana di tutti gli utenti dei servizi online.

La proposta di regolamento intende conseguire tali obiettivi nei seguenti modi:

- preservando in larga misura l'attuale regime di responsabilità per gli intermediari online, compreso il divieto di imporre obblighi generali di sorveglianza o di accertamento attivo dei fatti. Tale approccio si basa sull'attuale direttiva sul commercio elettronico[48] e mira a: i) tutelare in maniera proporzionata e adeguata il diritto alla libertà di espressione limitando gli incentivi alla rimozione di contenuti legali, e la libertà d'impresa, garantendo la proporzionalità degli sforzi richiesti agli intermediari online e proteggendo i loro legittimi utenti commerciali; ii) far fronte alle preoccupazioni di interesse pubblico legate alla diffusione di diversi tipi di contenuti illegali, garantendo che siano rapidamente rimossi dagli intermediari alle condizioni previste dalla legge;

- stabilendo una serie chiara e proporzionata di obblighi in materia di dovere di diligenza per gli intermediari online, al fine di garantire che i contenuti illegali siano contrastati in modo adeguato e trasparente e che gli utenti possano far valere i propri diritti. La proposta prevede inoltre una serie rigorosa di garanzie per le procedure di moderazione dei contenuti, compresi quelli basati su termini e condizioni stabiliti privatamente;

- imponendo alle piattaforme online di dimensioni molto grandi (che per il loro raggio d'azione hanno acquisito un ruolo sistemico centrale nel favorire il dibattito pubblico) l'obbligo di valutare e attenuare i rischi posti dai loro servizi, anche rispetto ad alcuni diritti fondamentali: rispetto della vita privata e della vita familiare, libertà di espressione e di informazione, non discriminazione e diritti del minore. Le strategie di attenuazione dei rischi devono inoltre tenere conto degli effetti potenzialmente negativi degli algoritmi di amplificazione dei contenuti delle piattaforme, quali sistemi di raccomandazione o sistemi pubblicitari. Le piattaforme online di dimensioni molto grandi sono inoltre soggette a una maggiore responsabilità, offrendo agli utenti maggiori possibilità di scelta nelle loro interazioni online e consentendo a revisori indipendenti e ricercatori abilitati di analizzare i loro sistemi.

Contrasto della disinformazione e regolamentazione della pubblicità politica online

La diffusione della disinformazione, della cattiva informazione e delle teorie complottistiche può determinare una polarizzazione dei dibattiti e mettere a rischio la salute, la sicurezza e l'ambiente. La disinformazione può inoltre ostacolare la capacità delle persone di adottare decisioni informate sulla base di informazioni corrette. In alcuni casi la disinformazione include discorsi che lo Stato può legittimamente limitare (come l'istigazione alla violenza e all'odio di stampo razzista e xenofobo). Tuttavia molto spesso è protetta dal diritto alla libertà di espressione, anche se non è fondata su prove scientifiche o eventi reali. Per quanto

[48] Direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico") (GU L 178 del 17.7.2000).

riguarda la libertà di espressione, gli Stati devono astenersi dalla censura. Per essere efficaci, le azioni volte a limitare la portata della disinformazione e delle teorie complottistiche devono essere associate alla promozione di un ambiente favorevole a un dibattito pubblico pluralistico e inclusivo. Ciò assume particolare importanza in relazione alle elezioni.

In tale contesto, nel periodo 2020-2021 la Commissione ha continuato a mettere a punto una serie di azioni volte a rendere l'ambiente online più trasparente, responsabilizzare i suoi attori e gli utenti e promuovere un dibattito democratico aperto online. Tali azioni includevano i) il sostegno a verificatori di fatti indipendenti e ricercatori accademici, in particolare attraverso l'**Osservatorio europeo dei media digitali**[49], ii) misure volte a migliorare l'alfabetizzazione mediatica e iii) il monitoraggio di un **codice di buone pratiche di autoregolamentazione sulla disinformazione**[50]. Sulla base dei risultati di tali attività di monitoraggio, la Commissione ha inoltre pubblicato orientamenti su come i firmatari attuali e futuri del codice di buone pratiche, comprese le applicazioni di messaggistica privata, il settore pubblicitario e altri portatori di interessi, potrebbero rafforzare la portata e l'applicazione del codice e garantire un quadro di monitoraggio più solido[51].

Per favorire il dibattito democratico, il **piano d'azione per la democrazia europea**[52] stabilisce misure volte a promuovere elezioni libere e regolari, rafforzare la libertà dei media e contrastare la disinformazione. Ciò include la proposta sulla trasparenza e sul targeting della pubblicità politica, adottata a novembre 2021[53] nel quadro delle misure volte a tutelare l'integrità elettorale e il dibattito democratico aperto. Secondo tali norme proposte, ogni messaggio pubblicitario di natura politica dovrebbe essere chiaramente etichettato come tale e contenere informazioni riguardanti, ad esempio, chi l'ha finanziato e quanto è costato. Le tecniche di targeting politico e di amplificazione dovrebbero essere spiegate pubblicamente e con un livello di dettaglio senza precedenti, e sarebbero vietate quando si utilizzano dati personali sensibili senza il consenso esplicito dell'interessato. Infine, il **nuovo piano d'azione per l'istruzione digitale (2021-2027)**[54] propone di elaborare orientamenti per insegnanti ed educatori volti a contrastare la disinformazione e promuovere l'alfabetizzazione digitale.

Proposta relativa a un nuovo regolamento sulla sicurezza generale dei prodotti

Per soddisfare ulteriori requisiti settoriali, a giugno 2021 la Commissione, nell'ambito del riesame del quadro dell'UE per la sicurezza dei prodotti, ha adottato e pubblicato una nuova proposta di **regolamento relativo alla sicurezza generale dei prodotti**[55]. Tale proposta, basata sulla proposta di legge sui servizi digitali, introdurrebbe requisiti aggiuntivi per i mercati online per quanto riguarda i prodotti non sicuri come categoria specifica di contenuti illegali. La proposta è attualmente all'esame dei colegislatori.

[49] EDMO – Uniti contro la disinformazione.
[50] Codice di buone pratiche sulla disinformazione | Plasmare il futuro digitale dell'Europa (europa.eu).
[51] https://ec.europa.eu/commission/presscorner/detail/it/ip_21_2585.
[52] Piano d'azione per la democrazia europea | Commissione europea (europa.eu).
[53] Proposta di regolamento relativo alla trasparenza e al targeting della pubblicità politica, COM(2021) 731 final.
[54] Piano d'azione per l'istruzione digitale (2021-2027) | Istruzione e formazione (europa.eu).
[55] Proposta di regolamento relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n. 1025/2012 e che abroga la direttiva 87/357/CEE del Consiglio e la direttiva 2001/95/CE del Parlamento europeo e del Consiglio, COM(2021) 346 final.

5. Tutela dei diritti fondamentali in caso di utilizzo dell'IA

L'uso delle tecnologie di intelligenza artificiale (IA) può avere importanti effetti positivi sulle nostre società. Può aumentare l'efficienza dei processi o stimolare l'innovazione e la ricerca. Può inoltre servire a promuovere una serie di diritti fondamentali, quali i diritti alla libertà di espressione e di informazione o all'assistenza sanitaria, e promuovere importanti questioni di interesse pubblico quali la sicurezza pubblica o la sanità pubblica.

D'altro canto, quando l'IA è utilizzata senza garanzie e controlli di qualità adeguati per automatizzare o sostenere i processi decisionali o per attività quali la sorveglianza, può anche violare i diritti delle persone. Tali violazioni possono verificarsi su larga scala, a seconda della diffusione dell'utilizzo di un sistema, e possono essere difficili da prevenire o rilevare quando il sistema di IA non è sufficientemente trasparente o le persone non sono a conoscenza del suo utilizzo. Ad esempio, l'utilizzo dell'IA per ricavare informazioni sulle persone può incidere sulla protezione dei dati e sulla vita privata. Le distorsioni negli algoritmi o nei dati di addestramento, come discriminazioni di genere o discriminazioni etniche o razziali, possono portare a situazioni ingiuste e discriminatorie. Se un sistema volto a stimare il potenziale successo sul lavoro è addestrato principalmente con dati riguardanti gli uomini, è probabile che fornisca risultati non ottimali se utilizzato per analizzare dati sulle donne, il che potrebbe portare a discriminazioni. L'uso dell'IA può incidere anche sui diritti relativi alla dignità umana, alla buona amministrazione, alla protezione dei consumatori, alla sicurezza e all'assistenza sociale, alla libertà di espressione, alla libertà di riunione, all'istruzione, all'asilo, alla contrattazione e all'azione collettive, alle condizioni di lavoro giuste ed eque, all'accesso all'assistenza preventiva, alla diversità culturale e linguistica, ai diritti alla protezione dei dati e al rispetto della vita privata nonché ai diritti dei gruppi vulnerabili come i minori. Se tali sistemi sono utilizzati nell'ambito delle attività di contrasto o giudiziarie, possono inoltre incidere sulla presunzione di innocenza e sul diritto a un processo equo e alla difesa. Inoltre, l'inaccessibilità o l'assenza di informazioni pertinenti sui sistemi automatizzati ostacola l'effettiva applicazione degli obblighi in materia di diritti fondamentali e l'accesso delle persone ai mezzi di ricorso.

Cos'è l'IA e quali sono le caratteristiche specifiche che possono comportare rischi?

- IA è il termine usato per indicare una serie di tecnologie che hanno subito un rapido sviluppo negli ultimi anni. Le funzioni di alcuni tipi di sistemi di IA seguono regole generate automaticamente e non programmate esplicitamente dalle persone. Ciò può talvolta portare a risultati sorprendenti ma può anche rappresentare una sfida. Sulla base della definizione di IA dell'OCSE, la proposta di legge sull'intelligenza artificiale definisce l'IA come un software sviluppato mediante apprendimento automatico, approcci basati sulla logica, sulla conoscenza o statistici e che può, per una serie di obiettivi definiti dall'uomo, generare risultati quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagisce.

- L'opacità (mancanza di trasparenza) e la complessità (funzionamento con molte componenti e processi diversi) di alcuni sistemi di IA rendono complicato individuare e dimostrare possibili violazioni delle leggi, comprese le disposizioni che garantiscono il rispetto dei diritti fondamentali, e risalire a eventuali errori o malfunzionamenti del sistema.

- Uno specifico sottoinsieme di applicazioni di IA può subire un continuo adattamento, anche durante l'utilizzo, e cambiare ed evolvere in modo imprevisto senza poter essere facilmente monitorato. Ciò comporta un certo grado di imprevedibilità che può incidere sulla sicurezza o sui diritti fondamentali.

- Le prestazioni autonome dei sistemi possono incidere sulla sicurezza, in quanto alcuni sistemi di IA richiedono un intervento umano minimo o nullo per lo svolgimento dei compiti.

- La dipendenza dai dati di alcuni sistemi e le possibili distorsioni incorporate negli algoritmi possono causare o aumentare distorsioni ed errori sistemici. Se questi sistemi non sono progettati, testati e utilizzati in modo adeguato, possono aggravare risultati negativi come le discriminazioni.

5.1 Situazione e azioni a livello degli Stati membri

Negli ultimi anni gli Stati membri dell'UE hanno cercato di affrontare le sfide poste dall'uso delle tecnologie di IA. Molti hanno elaborato strategie nazionali in materia di IA[56], in cui sottolineano la necessità di garantire il rispetto dei diritti fondamentali. Inoltre, gli Stati membri hanno elaborato o prevedono di elaborare orientamenti e norme etiche che aiutino coloro che utilizzano strumenti di IA a garantire la trasparenza, la tracciabilità e la solidità, a fare fronte a potenziali distorsioni e ad individuare modi efficaci per rispettare i loro obblighi di rispettare i diritti fondamentali. In alcuni casi gli orientamenti e le competenze sono elaborati da accademici[57] o gruppi di esperti istituiti a tale scopo[58].

Inoltre, agendo insieme a livello dell'UE, gli Stati membri hanno sottolineato la necessità di garantire che i diritti sanciti dalla Carta siano pienamente rispettati e hanno chiesto un riesame della legislazione pertinente esistente per renderla idonea a far fronte alle nuove opportunità e sfide poste dall'IA[59]. Ad ottobre 2020, 26 dei 27 Stati membri hanno adottato un documento intitolato "La Carta dei diritti fondamentali nel contesto dell'intelligenza artificiale e della trasformazione digitale"[60], in cui invitavano ad affrontare la questione dell'opacità, della complessità e della faziosità, nonché della relativa imprevedibilità e del comportamento parzialmente autonomo di taluni sistemi di IA, onde garantire il rispetto dei diritti fondamentali e agevolare l'applicazione delle norme giuridiche. Gli Stati membri hanno sottolineato l'importanza di coinvolgere vari portatori di interessi, compresi quelli della società civile, per trarre beneficio dalle loro competenze.

[56] Entro giugno 2021, 20 Stati membri e la Norvegia avevano pubblicato le rispettive strategie nazionali in materia di IA, mentre 7 Stati membri erano nella fase di stesura finale.
https://knowledge4policy.ec.europa.eu/ai-watch/national-strategies-artificial-intelligence_en.
[57] Ad esempio, ad aprile 2021 gli accademici dell'Università di Utrecht hanno elaborato un codice per una buona amministrazione pubblica digitale per le autorità olandesi basato sui diritti fondamentali.
https://www.rijksoverheid.nl/documenten/rapporten/2021/04/30/code-goed-digitaal-openbaar-bestuur.
[58] Un esempio in tal senso è la commissione tedesca per l'etica dei dati e le consulenze da essa prodotte nel 2019:
https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_node.html.
[59] Riunione del Consiglio europeo (19 ottobre 2017) – Conclusione EUCO 14/17, pag. 8. e Conclusioni relative al piano coordinato sull'intelligenza artificiale - (11 febbraio 2019) 6177/19, 2019.
[60] https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/it/pdf.

Al momento dell'adozione della presente relazione, nessuno Stato membro dell'UE aveva adottato una legislazione specifica per fare fronte alle sfide in materia di diritti fondamentali poste dall'uso dell'IA[61]. Sembra piuttosto che le autorità degli Stati membri si siano basate sulla normativa esistente. Nel 2017 un organo giurisdizionale italiano ha imposto al ministero dell'Istruzione italiano di rendere noto l'algoritmo decisionale automatizzato da esso utilizzato per la gestione della mobilità dei lavoratori, sulla base del diritto di accesso ai documenti, che garantisce anche il diritto a un ricorso effettivo[62]. Nel 2018 l'organo giurisdizionale nazionale finlandese per la non discriminazione e l'uguaglianza ha ritenuto discriminatorio un caso di valutazione del credito sulla base di statistiche relative al genere, al luogo di residenza, all'età e alla lingua, anziché basato su una valutazione individuale[63]. Nel febbraio 2020 un organo giurisdizionale olandese ha annullato la legge olandese che aveva istituito un sistema di rilevamento delle frodi sulla base del diritto fondamentale alla vita privata sancito dalla Convenzione europea dei diritti dell'uomo[64]. Per analizzare i dati raccolti da diverse autorità pubbliche per individuare le persone potenzialmente responsabili di frodi in materia di prestazioni sociali è stato utilizzato il sistema per l'indicazione del rischio (SyRi). L'organo giurisdizionale olandese ha ritenuto che l'uso di SyRi non fosse sufficientemente trasparente e che la sua ingerenza nel diritto alla vita privata non fosse proporzionata all'obiettivo del rilevamento delle frodi.

Questi esempi dimostrano che gli Stati membri hanno già dovuto affrontare le sfide poste dall'uso dell'IA in relazione ai diritti fondamentali. L'approccio proposto dalla Commissione alle sfide connesse all'IA mira a rafforzare l'effettiva tutela dei diritti fondamentali, promuovendo nel contempo l'innovazione nell'IA.

5.2 La proposta della Commissione di regolamentare l'IA ad alto rischio

Ad aprile 2021 la Commissione ha presentato una proposta di regolamento sull'intelligenza artificiale[65]. Gli obiettivi principali della proposta di legge sull'intelligenza artificiale sono la tutela dei diritti fondamentali e della sicurezza e la creazione di un mercato unico per i sistemi di IA affidabili. La proposta mira a garantire che i sistemi di IA ad alto rischio siano progettati e utilizzati nel rispetto dei diritti fondamentali e che le autorità e gli organi giurisdizionali nazionali competenti possano indagare in modo più efficace e fare fronte ad eventuali violazioni degli obblighi in materia di diritti fondamentali.

La proposta segue un approccio basato sul rischio. Alcuni sistemi di IA sono del tutto vietati, come quelli che utilizzano tecniche subliminali e quelli utilizzati dalle autorità pubbliche per il punteggio sociale, in quanto violano i valori dell'UE. È altresì vietato l'uso di sistemi di

[61] La Finlandia ha riferito che sono in corso i lavori per elaborare un progetto di proposta legislativa sul processo decisionale amministrativo automatizzato entro la fine del 2021. Gli esempi di azioni degli Stati membri (legislazione, finanziamenti o altro) inclusi nella presente relazione mira a illustrare diversi tipi di azioni. Non è possibile citare tutte le iniziative relative a ciascun argomento e la selezione si basa in larga misura sulle informazioni presentate dagli Stati membri a giugno 2021.
[62] T.A.R., Roma, Sez. III-bis, 22 marzo 2017, n° 3769.
[63] https://www.yvtltk.fi/material/attachments/ytaltk/tapausselosteet/45LI2c6dD/YVTltk-tapausseloste-_21.3.2018-luotto-moniperusteinen_syrjinta-S-en_2.pdf.
[64] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878.
[65] Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM/2021/206 final.

identificazione biometrica remota in spazi accessibili al pubblico a fini di attività di contrasto, a meno che non si applichino eccezioni e garanzie chiaramente definite.

I sistemi di IA ad alto rischio dovranno rispettare una serie di requisiti e seguire procedure di valutazione della conformità prima di essere immessi sul mercato o messi in servizio. Tali requisiti garantiscono un'adeguata documentazione e controllo dei sistemi di IA ad alto rischio, nonché un'adeguata qualità dei dati, tracciabilità, sorveglianza umana, solidità, accuratezza e cibersicurezza. Si applicheranno nei casi in cui i sistemi di IA siano utilizzati in settori critici, quali l'identificazione biometrica, l'istruzione, l'occupazione, i servizi pubblici e privati essenziali quali i crediti o le prestazioni assistenziali, le attività di contrasto, la migrazione e il controllo delle frontiere e le attività giudiziarie. Anche i sistemi di IA che consistono in componenti di sicurezza di determinati prodotti regolamentati (ad esempio macchinari, dispositivi medici) saranno soggetti agli stessi requisiti e dovranno essere controllati prima di poter essere immessi sul mercato dell'UE o messi in servizio.

La proposta garantisce che gli utenti dei sistemi di IA, come le imprese che interagiscono con i clienti o le autorità pubbliche che adottano decisioni, ricevano informazioni adeguate dagli sviluppatori dei sistemi per garantire un uso adeguato delle loro applicazioni e consentire loro di adempiere agli obblighi previsti dal diritto in materia di diritti fondamentali.

Qualora si verifichino violazioni dei diritti fondamentali attraverso l'uso di sistemi di IA, la trasparenza e la tracciabilità dei sistemi di IA, associate a rigorosi controlli ex post da parte delle autorità competenti, garantiranno la possibilità di un ricorso efficace per gli interessati. Le autorità di controllo incaricate di far rispettare i diritti fondamentali, quali le autorità per la protezione dei dati, gli organismi per la parità o gli organismi per la tutela dei consumatori, avranno accesso a tutta la documentazione relativa ai sistemi di IA ad alto rischio che rientrino nel loro mandato. Potranno cooperare con le autorità di vigilanza del mercato per testare, se necessario, i rispettivi sistemi di IA.

Nel caso di sistemi di IA specifici, gli obblighi di trasparenza nei confronti delle persone interessate ridurranno al minimo il rischio di manipolazione, in particolare nel caso di chat bot (programmi informatici in grado di rispondere a domande in una chat online) o di *deepfake* (immagini generate o manipolate in modo artificiale, contenuti audio o video che somigliano a persone, oggetti, luoghi o altri soggetti o eventi esistenti e che appaiono falsamente autentici o veritieri). Le persone dovrebbero inoltre essere informate quando si utilizzano sistemi di riconoscimento delle emozioni o di classificazione biometrica, il che le aiuterebbe a far valere i propri diritti ai sensi della legislazione vigente in materia di protezione dei dati.

La proposta è attualmente all'esame dei colegislatori.

5.3 Interazione con la legislazione settoriale - L'esempio del merito creditizio e del credit scoring

La proposta di legge sull'intelligenza artificiale andrà di pari passo con altre normative che stabiliscono norme sostanziali per l'uso dei sistemi di IA in contesti chiaramente mirati. Ad esempio, i fornitori di crediti utilizzano spesso tecniche decisionali automatizzate, compresi i sistemi di IA, per le valutazioni del merito creditizio o per il credit scoring. Tali fornitori si basano su dati diversi, molti dei quali non vengono forniti dal consumatore o non sono per loro noti. Ciò solleva preoccupazioni in merito alla protezione dei dati personali, alla

discriminazione diretta o indiretta[66] e alla protezione dei consumatori[67]. La **direttiva relativa al credito ai consumatori[68]** e la **direttiva in merito al credito ipotecario[69]** contengono disposizioni sulla valutazione del merito creditizio. A giugno 2021 la Commissione ha adottato una **nuova proposta di direttiva relativa al credito ai consumatori** che abroga e sostituisce l'attuale direttiva sul credito ai consumatori. Essa propone norme relative alla concessione di crediti ai consumatori, in base alle quali gli Stati membri dovranno garantire la documentazione delle procedure e delle informazioni utilizzate nell'ambito delle valutazioni del merito creditizio. Inoltre, le valutazioni dovranno basarsi su informazioni pertinenti e accurate sulle circostanze economiche e finanziarie (ad esempio entrate e spese) e non dovrebbero basarsi su dati come quelli dei social media. I consumatori avranno inoltre il diritto di ricevere una spiegazione su come è stata presa una decisione sul relativo merito creditizio, di esprimere il proprio punto di vista e ottenere l'intervento di un operatore, il che rispecchia i principi del regolamento generale sulla protezione dei dati (GDPR)[70] relativi al processo decisionale automatizzato. La nuova proposta comprende anche un articolo sulla non discriminazione, in cui si specifica che le condizioni da soddisfare per la concessione di un credito non devono discriminare i consumatori che risiedono legalmente nell'Unione in base alla cittadinanza o al luogo di residenza o a qualsiasi altro motivo di cui all'articolo 21 della Carta dei diritti fondamentali dell'Unione europea. La proposta è attualmente all'esame dei colegislatori.

5.4 Competenze

Quando si utilizzano sistemi di IA, i lavoratori devono essere adeguatamente qualificati per garantire il rispetto dei diritti fondamentali e un'adeguata sorveglianza umana. Le autorità di vigilanza avranno inoltre bisogno di personale con competenze tecniche specifiche per adempiere efficacemente ai loro mandati. A settembre 2020 la Commissione ha adottato un **piano d'azione per l'istruzione digitale** per il periodo 2021-2027[71] che mira a promuovere le competenze digitali, anche in relazione all'IA[72], e include lo sviluppo di orientamenti etici nel settore dell'IA e dei dati nell'istruzione e nell'apprendimento. Inoltre, tutti gli Stati membri che hanno adottato strategie nazionali in materia di IA hanno integrato nelle loro strategie una componente sulle competenze, ad esempio attraverso riforme dei sistemi educativi per

[66] Ad esempio, ad aprile 2019 il mediatore finlandese incaricato della protezione dei dati ha ordinato alla società di credito finanziario Svea Ekonomi di correggere le sue pratiche di valutazione del merito creditizio, in quanto giudicava che un limite massimo di età non fosse un fattore accettabile, poiché l'età non descrive la solvibilità o la disponibilità a sostenere i costi.

[67] Relazione sulla valutazione d'impatto che accompagna la proposta di direttiva relativa ai contratti di credito ai consumatori che abroga e sostituisce la direttiva 2008/48/CE, COM(2021) 347 final.

[68] Direttiva 2008/48/CE del Parlamento europeo e del Consiglio, del 23 aprile 2008, relativa ai contratti di credito ai consumatori e che abroga la direttiva 87/102/CEE (GU L 133 del 22.5.2008, pag. 66).

[69] Direttiva 2014/17/UE del Parlamento europeo e del Consiglio, del 4 febbraio 2014, in merito ai contratti di credito ai consumatori relativi a beni immobili residenziali e recante modifica delle direttive 2008/48/CE e 2013/36/UE e del regolamento (UE) n. 1093/2010 (Testo rilevante ai fini del SEE) (GU L 60 del 28.2.2014, pag. 34).

[70] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[71] Piano d'azione per l'istruzione digitale (2021-2027) | Istruzione e formazione (europa.eu).

[72] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan/action-8_it.

rafforzare il pensiero computazionale o iniziative volte ad adeguare le politiche di apprendimento permanente e di riqualificazione[73].

6. Colmare il divario digitale

Il fatto di essere connessi e competenti a livello digitale consente di partecipare attivamente alla società. Sono sempre più numerose le attività essenziali che si spostano online: dalla ricerca di un impiego al telelavoro, ai corsi di studio, all'interazione con una pubblica amministrazione o alla prenotazione di una visita medica. Ma non tutti i cittadini sono online. Il fatto di non essere online può incidere sull'esercizio dei propri diritti. Ad esempio, può incidere sui diritti dei cittadini in una società democratica, compreso il diritto alla libertà di espressione e di informazione, e sul loro diritto di candidarsi alle elezioni comunali, dal momento che le campagne politiche sono condotte sempre più spesso online. La pandemia di COVID-19 ha aggravato queste difficoltà di accesso ai servizi pubblici per coloro che non dispongono delle attrezzature o delle conoscenze digitali necessarie, data la chiusura degli uffici e la richiesta di comunicare con le amministrazioni nazionali online.

Questo fenomeno è spesso definito "divario digitale". Ancora oggi il 46 % degli europei non dispone di competenze digitali di base[74]. Ciò è riconosciuto dal **pilastro europeo dei diritti sociali**, che include le comunicazioni digitali tra i servizi essenziali a cui tutti dovrebbero avere accesso e chiede misure di sostegno per coloro che ne hanno bisogno[75]. Coloro che non dispongono di un accesso regolare a Internet o delle competenze necessarie per usufruire di tali servizi, o che non possono accedere a un prodotto o servizio digitale a causa di disabilità fisiche o cognitive, rischiano sempre più di essere esclusi e incontrano difficoltà nell'esercizio dei loro diritti.

Nel caso dei servizi pubblici accessibili esclusivamente con mezzi digitali, chi non è connesso può trovarsi nell'impossibilità di esercitare i propri diritti o avrebbe bisogno di aiuto per farlo. A titolo di esempio, l'*Haut Conseil du Travail*, organo consultivo del ministero francese degli Affari sociali, stima che una persona su cinque in Francia abbia difficoltà a completare le procedure amministrative online e avverte che la digitalizzazione può compromettere il principio della parità di accesso ai servizi pubblici se non vengono mantenuti mezzi di accesso alternativi[76]. Analogamente, dato che sempre più attività economiche hanno una componente digitale, l'esercizio del diritto di accesso ai servizi di interesse economico generale è diventato sempre più subordinato all'accesso a Internet. I minori che non dispongono di un dispositivo connesso a casa hanno difficoltà a partecipare alle attività scolastiche da remoto, il che incide sui diritti del minore e sul diritto all'istruzione. Inoltre, nei casi in cui i siti web e le applicazioni mobili non sono adeguati alle

[73] https://knowledge4policy.ec.europa.eu/ai-watch/national-strategies-artificial-intelligence_en.
[74] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020DC0624 e Statistiche | Eurostat (europa.eu).
[75] Il pilastro europeo dei diritti sociali in 20 principi | Commissione europea (europa.eu), cfr. principio 20.
[76] https://solidarites-sante.gouv.fr/IMG/pdf/pourquoi_et_comment_les_travailleurs_sociaux_se_saisissent_des_outils_numeriques.pdf, pag. 4.

esigenze delle persone con disabilità, il diritto di queste ultime all'integrazione potrebbe essere ostacolato.

Alla luce delle sfide poste dal divario digitale, gli Stati membri e la Commissione stanno attuando una serie di misure volte a garantire che nessuno sia lasciato indietro. Come annunciato nel **piano d'azione sul pilastro europeo dei diritti sociali**[77], nel 2022 la Commissione pubblicherà una relazione sull'accesso ai servizi essenziali, che riguarderà anche l'accesso alle comunicazioni digitali, presentando una panoramica della situazione nell'UE-27 e una mappatura delle misure nazionali e dell'UE esistenti e delle buone prassi a sostegno dell'accesso per le persone bisognose.

6.1 Riduzione generale del divario digitale

Il fatto che durante la pandemia molte attività si siano svolte online non rappresenta solo una sfida, ma anche un'opportunità. Gli Stati membri hanno sviluppato progetti che l'UE finanzierà per aiutare l'economia a riprendersi dalla recessione causata dalla pandemia. Tali progetti comprendono misure volte a colmare il divario digitale e a conseguire diritti digitali inclusivi, nonché ad affrontare la digitalizzazione del lavoro. A titolo di esempio è possibile citare due piani nazionali. La **Romania** prevede di investire nella creazione di contenuti educativi e risorse accessibili, quali video e lezioni interattive, e di sviluppare programmi accessibili di alfabetizzazione digitale per gli studenti con disabilità. La **Germania** intende contribuire all'acquisto di dispositivi digitali per gli insegnanti a livello nazionale. Creerà inoltre una piattaforma per l'apprendimento digitale permanente e presterà particolare attenzione al sostegno delle persone formalmente meno qualificate.

Più in generale, esistono numerose iniziative promettenti in diversi Stati membri[78]. A febbraio 2021 il **Belgio** ha presentato un invito pubblico a presentare progetti a sostegno delle imprenditrici colpite dalla pandemia di COVID-19, fornendo anche linee guida relative alla digitalizzazione. Il Belgio sta inoltre investendo in organizzazioni locali che mirano ad aumentare le competenze digitali dei giovani in situazioni di precarietà economica.

Il **Portogallo** sta mobilitando giovani volontari affinché contribuiscano a educare gli adulti sulla transizione digitale, sulla base di una rete nazionale di 1 500 centri di formazione e di una serie di strumenti e risorse gratuiti. Il programma per l'inclusione digitale, di cui dovrebbe beneficiare un milione di persone, sarà attuato in collaborazione con le autorità e le organizzazioni locali[79].

Secondo una logica analoga all'iniziativa WiFi4EU[80], l'**Italia** sovvenziona l'accesso a Internet per determinate persone e ha avviato il progetto "Piazza Wifi Italia"[81] che consente a oltre 400 000 persone di collegarsi gratuitamente e con facilità a una rete Wi-Fi diffusa in

[77] Piano d'azione sul pilastro europeo dei diritti sociali (europa.eu).
[78]Poiché nella presente relazione non è possibile citare tutte le iniziative, la seguente selezione mira a illustrare diverse tipologie di azioni, basandosi sulle informazioni presentate dagli Stati membri nel giugno 2021.
[79] Resolução do Conselho de Ministros n.º 30/2020 - DRE.
[80] https://digital-strategy.ec.europa.eu/it/activities/wifi4eu.
[81] https://www.wifi.italia.it/it/.

tutto il paese attraverso un'app dedicata. A marzo 2020 il progetto è stato esteso alle strutture sanitarie, compresi gli ospedali.

Poiché è probabile che le infrastrutture digitali continuino a evolversi, l'UE si è attivata in una serie di settori per migliorare la connettività. L'obiettivo principale in materia di connettività nel **decennio digitale** è che ogni famiglia europea abbia accesso alla copertura internet ad alta velocità entro il 2025 e alla connettività Gigabit entro il 2030[82]. A marzo 2021 la Commissione e gli Stati membri hanno concordato un **pacchetto di strumenti per la connettività** volto a promuovere la diffusione delle reti digitali e facilitare l'accesso allo spettro 5G. La revisione della direttiva sulla riduzione dei costi della banda larga, prevista per il 2022, mira a sostenere ulteriormente la diffusione delle reti digitali riducendo gli oneri amministrativi e i costi e la velocità di tale diffusione. Inoltre, la **visione a lungo termine della Commissione per le zone rurali**[83] di giugno 2021 mira a colmare il divario tra città e zone rurali consentendo l'accesso alla connettività internet veloce, al 5G (anche mediante finanziamenti dell'UE[84]) e alla tecnologia digitale, nonché rafforzando le competenze digitali. La connettività a banda larga ad alta velocità è un fattore chiave per la transizione digitale e la ripresa post COVID-19. La Commissione si è impegnata a ridurre i divari digitali in termini di accessibilità nelle zone rurali e l'UE investirà in infrastrutture di rete, in una norma per la trasmissione di dati senza fili e nella fibra ottica per garantire che tutti nell'UE abbiano accesso a infrastrutture di connettività digitale efficienti sotto il profilo energetico e adeguate alle esigenze future.

6.2 Amministrazione pubblica

La tecnologia digitale consente alle persone di beneficiare di un accesso più ampio ai servizi pubblici e alle informazioni che possono aiutarle a gestire la propria vita quotidiana ed esercitare i propri diritti, in particolare la libertà di creare e fornire servizi. A partire dalla **dichiarazione di Malmö**, firmata in occasione di un vertice tenutosi in Svezia nel 2009, gli Stati membri dell'UE hanno compiuto progressi costanti nella modernizzazione delle pubbliche amministrazioni[85]. La **dichiarazione di Tallinn** del 2017 ha incentivato la digitalizzazione dei servizi pubblici destinati alle persone e dei servizi pubblici transfrontalieri destinati alle imprese[86]. Più di recente, la **dichiarazione di Berlino** di dicembre 2020 ha incluso tra gli impegni degli Stati membri le misure da adottare per la tutela dei diritti fondamentali online[87] e la **dichiarazione di Lisbona** di giugno 2021 mira a

[82] Comunicazione della Commissione "Bussola per il digitale 2030: il modello europeo per il decennio digitale", COM(2021) 118 final.
[83] Una visione a lungo termine per le zone rurali dell'UE | Commissione europea (europa.eu).
[84] I finanziamenti del Fondo europeo di sviluppo regionale, del Fondo europeo agricolo per lo sviluppo rurale, del meccanismo per collegare l'Europa 2 e del dispositivo per la ripresa e la resilienza saranno disponibili per conseguire gli obiettivi di connettività dell'UE per il 2025.
[85] https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf.
[86] https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration.
[87] https://ec.europa.eu/isa2/news/eu-member-states-sign-berlin-declaration-digital-society_it.

garantire che "nessuno sia lasciato indietro". Gli Stati membri si sono inoltre impegnati nella digitalizzazione della giustizia[88].

Gli Stati membri stanno adottando approcci diversi per garantire l'accesso ai servizi pubblici, cercando di ridurre il divario digitale e soddisfacendo nel contempo le esigenze di questa era digitale. Ad esempio, la **Francia** ha scelto di mantenere diverse modalità di garantire l'accesso ai servizi pubblici al fine di evitare eventuali ostacoli. Le persone non devono contattare l'amministrazione obbligatoriamente per via elettronica. La **Danimarca** ha seguito un percorso diverso, definendo una strategia "digitale per default", e nel 2014 ha reso obbligatorio l'uso di mezzi elettronici per qualsiasi contatto con l'amministrazione. Per colmare il divario digitale, lo Stato finanzia misure quali assistenza personalizzata gratuita nelle biblioteche[89], assistenza per l'acquisto di attrezzature e contributi per gli abbonamenti a Internet. Analogamente, nei **Paesi Bassi** il governo e le biblioteche locali hanno avviato l'iniziativa "Information Point Digital Government" nell'ambito della quale un dipendente della biblioteca formato risponde alle domande delle persone aiutandole con i tradizionali servizi pubblici digitali, quali le dichiarazioni dei redditi e i servizi sociali, nonché con i servizi più recenti come le app relative alla COVID-19.

6.3 Assistenza sanitaria

La pandemia ha causato un aumento dell'assistenza sanitaria online, ad esempio tramite consulti virtuali o applicazioni e software sviluppati a fini diagnostici o terapeutici. Per alcuni, come ad esempio le persone che vivono nelle zone rurali o nelle piccole isole, questa tendenza rende più facile ricevere assistenza medica, mentre per altri rappresenta un nuovo ostacolo. Per coloro che non hanno l'accesso o le competenze necessari, le misure volte a colmare il divario digitale possono migliorare la situazione. Ad esempio, la **Polonia** ha introdotto l'account Internet del paziente, uno strumento online che consente ai pazienti di accedere alle informazioni sulle proprie cure mediche passate, attuali o programmate e di gestire una serie di pratiche (prescrizione elettronica, storico delle visite, impegnativa elettronica, congedi di malattia elettronici e diritti) senza doversi recare di persona in una struttura sanitaria.

6.4 Istruzione

Diversi Stati membri dispongono di politiche e programmi volti a promuovere l'accesso alla tecnologia e rafforzare le competenze digitali nel contesto dell'istruzione formale. La **Grecia**, ad esempio, fornisce agli alunni e studenti bisognosi dei buoni per l'acquisto di attrezzature quali tablet o computer ed eroga programmi di formazione pertinenti attraverso una *Digital Skills Academy* virtuale, lanciata nel 2020.

[88] I progressi compiuti in questo settore sono illustrati nella relazione della Commissione sullo Stato di diritto 2021: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52021DC0700&from=EN.
Cfr. anche la comunicazione della Commissione sulla digitalizzazione della giustizia nell'Unione europea, COM(2020) 710 final e relativo SWD(2020) 540 del 2 dicembre 2020.

[89] Tale assistenza viene fornita anche in altri contesti, ma al fine di illustrare l'approccio sono sufficienti solo alcuni esempi. L'obiettivo della presente relazione non è una mappatura esaustiva delle misure, ma piuttosto una panoramica delle idee e degli approcci.

A livello dell'UE, il **piano d'azione per l'istruzione digitale**[90] (2021-2027), varato a settembre 2020, ha definito una visione strategica a lungo termine per una trasformazione digitale sostenibile e inclusiva nell'ambito dell'istruzione e dell'apprendimento. Promuove il diritto di accesso a un'istruzione digitale di alta qualità per tutti e la parità di accesso alle infrastrutture, mirando in particolare a incoraggiare la partecipazione delle ragazze e delle donne alle discipline STEM (scienza, tecnologia, ingegneria e matematica).

6.5 Inserimento delle persone con disabilità

Il **codice europeo delle comunicazioni elettroniche**[91] garantisce un accesso e una scelta equivalenti in relazione ai servizi di comunicazione elettronica per gli utenti finali con disabilità, favorendone la partecipazione alla società digitale. L'**atto europeo sull'accessibilità**[92] entrerà in vigore nel 2025 ed estenderà l'inclusione delle persone con disabilità e degli anziani nel mondo digitale rendendo più accessibile una serie di prodotti e servizi fondamentali sia del settore privato che di quello pubblico. La **direttiva sull'accessibilità del web** del 2016[93] impone agli Stati membri di garantire che i siti web e le applicazioni mobili degli enti pubblici siano accessibili alle persone con disabilità, come le persone con disabilità visive, uditive o motorie. In tal modo promuove la libertà di espressione e di informazione, il diritto all'istruzione, la libertà professionale e il diritto al lavoro, la non discriminazione, l'integrazione delle persone con disabilità, l'accesso ai servizi di interesse economico generale, il diritto di accesso ai documenti, il diritto di circolare e soggiornare liberamente nel territorio dell'Unione, la libertà di stabilimento e la libera prestazione dei servizi.

La direttiva può essere attuata in modi diversi. Ad esempio, la **Slovenia** ha modernizzato il portale statale di e-government in modo tale che possa essere utilizzato da non vedenti e ipovedenti, non udenti e ipoudenti, persone affette da dislessia e utenti con problemi di tipo cognitivo. Ad esempio, le descrizioni testuali delle procedure sono corredate da brevi video che includono interpretazioni nella lingua dei segni. In **Grecia**, durante la pandemia, i libri scolastici digitali sono stati adattati in modo tale che potessero accedervi le persone affette da qualsiasi tipo di disabilità.

7. Tutelare le persone che lavorano attraverso le piattaforme digitali

Le piattaforme online includono un'ampia scelta di mercati, social media, punti vendita di contenuti creativi, app store, siti di confronto dei prezzi, piattaforme per l'economia collaborativa e motori di ricerca, che favoriscono l'interazione tra utenti e imprese. Le piattaforme di lavoro digitali, in qualità di sottoinsieme distinto di piattaforme online, si sono rivelate un elemento caratteristico dell'economia digitale.

[90] Piano d'azione per l'istruzione digitale (2021-2027) | Istruzione e formazione (europa.eu).
[91] Direttiva (UE) 2018/1972 che istituisce il codice europeo delle comunicazioni elettroniche (rifusione) (GU L 321 del 17.12.2018).
[92] Direttiva (UE) 2019/882 sui requisiti di accessibilità dei prodotti e dei servizi (GU L 151 del 7.6.2019).
[93] Direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici (GU L 327 del 2.12.2016).

Il lavoro su piattaforma digitale ha creato nuove opportunità economiche per le persone, consentendo loro, ad esempio, di svolgere attività a tempo parziale e di accedere al mercato del lavoro in generale. Nel contempo rischia di compromettere diritti fondamentali, tra cui la protezione dei dati personali, della vita privata, del diritto dei lavoratori all'informazione e alla consultazione, del diritto alla negoziazione e all'azione collettive e a condizioni di lavoro giuste ed eque. Tra i 28 milioni di persone che, secondo le stime, lavorano attraverso le piattaforme di lavoro digitali, potrebbero esserci fino a 5,5 milioni di "falsi autonomi"[94]: sebbene i loro contratti con le piattaforme attraverso le quali lavorano li descrivano come lavoratori autonomi, in realtà sono soggetti a controllo e vigilanza, che sono caratteristici dello status di "lavoratore". I modelli operativi basati su algoritmi pongono a loro volta sfide quali la mancanza di informazioni e di consultazioni con le persone che lavorano attraverso le piattaforme digitali e i loro rappresentanti sul modo in cui gli algoritmi sono utilizzati e incidono sulle condizioni del lavoro su piattaforma digitale. Inoltre i mezzi di ricorso sono insufficienti e le responsabilità per quanto riguarda l'uso degli algoritmi sono poco chiare.

Lavoro su piattaforma digitale

Il lavoro su piattaforma digitale coinvolge di norma tre parti: la **piattaforma**, la **persona che lavora attraverso la piattaforma** e il **cliente** (privati o imprese). In alcuni casi potrebbe essere coinvolta anche una quarta parte, come ad esempio i ristoranti che consegnano cibo.

Le piattaforme di lavoro digitali si definiscono solitamente come intermediari e descrivono il rapporto tra le parti come lavoro autonomo. Le attività svolte sulle piattaforme di lavoro digitali possono variare da attività complesse, come la programmazione informatica e la progettazione grafica, ad attività semplici come l'inserimento di tag nelle immagini.

La presidente della Commissione Ursula von der Leyen ha annunciato nei suoi orientamenti politici la necessità di migliorare le condizioni di lavoro nell'ambito del lavoro su piattaforma digitale[95]. Questa esigenza è stata ulteriormente evidenziata dalla crisi della COVID-19 e dall'accelerazione dell'adozione dei modelli operativi delle piattaforme. Una recente risoluzione del Parlamento europeo[96] sottolinea che il lavoro su piattaforma digitale ha sollevato preoccupazioni circa la precarietà e le cattive condizioni di lavoro, l'assenza di una protezione sociale adeguata o le difficoltà di accesso alla stessa, redditi frammentati e imprevedibili e l'assenza di misure in materia di salute e sicurezza sul lavoro. Chiede un'azione decisa da parte dell'UE per fare fronte all'errata classificazione della situazione occupazionale e migliorare la trasparenza nell'uso degli algoritmi, anche per i rappresentanti dei lavoratori.

[94] Cfr. la relazione sulla valutazione d'impatto che accompagna la proposta di direttiva relativa al miglioramento delle condizioni di lavoro nell'ambito del lavoro su piattaforma digitale, SWD(2021) 396 final.
[95] COM(2021) 762.
[96] Risoluzione del Parlamento europeo del 16 settembre 2021 su condizioni di lavoro eque, diritti e protezione sociale per i lavoratori delle piattaforme - Nuove forme di occupazione legate allo sviluppo digitale (2019/2186(INI)).

7.1 Situazione e azioni a livello degli Stati membri

Al fine di prevenire la concorrenza sleale a danno dei lavoratori e una corsa al ribasso nelle pratiche occupazionali e nelle norme sociali, l'UE ha creato una soglia minima dei diritti del lavoro che si applica ai lavoratori in tutti gli Stati membri. Il corpus legislativo dell'UE in materia di lavoro e affari sociali è cresciuto nel corso degli anni. Inoltre, le risposte nazionali alle sfide poste dal lavoro su piattaforma variano da uno Stato membro all'altro. Alcuni hanno adottato una legislazione nazionale per migliorare le condizioni di lavoro o l'accesso alla protezione sociale nell'ambito del lavoro su piattaforma. Gli organi giurisdizionali si sono pronunciati sulla questione dell'errata classificazione della situazione occupazionale in un numero significativo di Stati membri. In alcuni Stati membri le parti sociali e le imprese di piattaforme hanno avviato trattative sui contratti collettivi.

Nel 2016 la **Francia** ha adottato una legislazione che prevede diritti sociali e lavorativi per le persone che lavorano attraverso le piattaforme digitali indipendentemente dal settore di attività economica, mediante la revisione del codice del lavoro. La legge, che si applica ai lavoratori autonomi dipendenti dal punto di vista tecnologico ed economico, consente l'accesso a un regime di assicurazione volontaria contro gli infortuni sul lavoro, obbliga le piattaforme a pagare i premi assicurativi o a fornire un'assicurazione collettiva ai propri lavoratori e garantisce il diritto di intraprendere azioni collettive e proseguire i percorsi di studio. Inoltre, il supremo organo giurisdizionale per le questioni riguardanti il lavoro privato (la Corte di cassazione) ha sottolineato in due sentenze che ai lavoratori delle piattaforme nel settore del ride-hailing deve essere riconosciuto lo status di lavoratore nel caso in cui la piattaforma possa impartire e far rispettare delle istruzioni[97]. Tuttavia il dibattito sullo status effettivo delle persone che lavorano attraverso le piattaforme digitali prosegue anche in altri settori.

In **Italia**, nel 2019, la regione Lazio ha adottato una normativa[98] volta a migliorare le condizioni di lavoro e la protezione sociale per tutti i lavoratori delle piattaforme, indipendentemente dalla loro situazione occupazionale. Tale normativa prevede garanzie per gli infortuni sul lavoro, un'adeguata formazione in materia di sicurezza, un'assicurazione per la responsabilità civile e gli infortuni e vieta inoltre il pagamento a cottimo. Nel 2019 l'Italia ha inoltre adottato una normativa nazionale volta a migliorare le condizioni di lavoro dei rider autonomi per la consegna di cibo[99]. Inoltre, a luglio 2021 il Garante italiano per la protezione dei dati personali ha condannato Deliveroo Italy a pagare una sanzione di 2,5 milioni di EUR per la scarsa trasparenza nell'uso degli algoritmi e la raccolta sproporzionata di dati relativi ai lavoratori. L'autorità ha riscontrato violazioni di alcune disposizioni del regolamento generale sulla protezione dei dati e della normativa nazionale sulla tutela della vita privata, dello Statuto dei lavoratori italiano e della summenzionata normativa a tutela dei lavoratori[100].

[97] Take Eat Easy (18 novembre 2018, causa 17-20.079) e Uber (4 marzo 2020, causa 19-13.316).
[98] Regione Lazio, Legge Regionale 12 aprile 2019, n. 4, disponibile online.
[99] L. 2 novembre 2019, n. 128, Conversione in legge, con modificazioni, del decreto-legge 3 settembre 2019, n. 101, disponibile online.
[100] Decisione del Garante italiano per la protezione dei dati personali, disponibile online.

A maggio 2021 la **Spagna** ha adottato una normativa che introduce la presunzione che le persone che lavorano attraverso le piattaforme digitali per la consegna di cibo e pacchi siano considerate lavoratori, spostando sulle piattaforme l'onere della prova per dimostrare il contrario[101]. Inoltre, tale legge obbliga le piattaforme a fornire ai sindacati informazioni sulla gestione algoritmica, compresi il monitoraggio digitale delle prestazioni e l'assegnazione automatizzata degli ordini. Tale legge stabilisce che tutte le imprese (non solo le piattaforme di consegna) debbano informare i propri lavoratori in merito ai parametri e alle norme su cui si basano i sistemi automatizzati, che possono incidere sulle condizioni di lavoro, sull'accesso e sul mantenimento del posto di lavoro.

La **Germania** ha pubblicato documenti strategici sul futuro del lavoro, riguardanti l'inclusione dei lavoratori autonomi su piattaforma digitale nei regimi pensionistici e assicurativi e il miglioramento della loro assicurazione contro gli infortuni sul lavoro.

A novembre 2020 il **Portogallo** ha a sua volta pubblicato un documento strategico sul futuro del lavoro, relativo alla creazione di una presunzione legale sullo status delle persone che lavorano attraverso le piattaforme digitali, alle modalità per aumentare la protezione sociale per i lavoratori autonomi e per promuovere la rappresentanza collettiva dei lavoratori delle piattaforme. Nel 2018 il Portogallo ha adottato una normativa sul trasporto individuale a pagamento di passeggeri, che fissa limiti all'orario di lavoro dei conducenti[102].

7.2 Un approccio comune dell'UE

Alla luce degli approcci sviluppati dagli Stati membri per fare fronte alle diverse sfide connesse al lavoro su piattaforma digitale, vi è un rischio di frammentazione tra le diverse iniziative legislative nazionali. La Commissione ha individuato una serie di sfide relative al lavoro su piattaforma digitale e ha consultato le parti sociali europee in due fasi in merito alla necessità di un'iniziativa sul lavoro su piattaforma digitale e sulla sua possibile direzione. Le parti sociali europee concordano sulle sfide da affrontare, ma hanno opinioni contrastanti circa la necessità di un'azione concreta a livello dell'UE. La Commissione ha inoltre tenuto scambi con molti portatori di interessi, tra cui riunioni dedicate e bilaterali con le imprese delle piattaforme, le associazioni dei lavoratori delle piattaforme, i sindacati, i rappresentanti degli Stati membri, gli esperti del mondo accademico e delle organizzazioni internazionali e i rappresentanti della società civile[103]. La Commissione ha proposto una direttiva volta a migliorare le condizioni di lavoro dei lavoratori delle piattaforme a livello dell'UE, garantendo la corretta determinazione della loro situazione occupazionale, promuovendo la trasparenza, l'equità e la responsabilità nella gestione algoritmica del lavoro su piattaforma digitale e migliorando la trasparenza del lavoro su tali piattaforme, anche in ambito transfrontaliero, favorendo nel contempo le condizioni per la crescita sostenibile delle piattaforme di lavoro digitali nell'Unione.

[101] Decreto legge reale 9/2021 dell'11 maggio, disponibile online.
[102] Lei n°45/2018, *Regime jurídico da atividade de trasporte individual e remunderado de passageiros em veículos descaracterizadosa partir de plataforma electrónica*, disponibile online.
[103] Cfr. l'allegato A.3.1 della valutazione d'impatto che accompagna la proposta di direttiva relativa al miglioramento delle condizioni di lavoro nell'ambito del lavoro su piattaforma digitale, SWD(2021) 396 final.

8. Supervisione della sorveglianza digitale

La protezione dei dati e la vita privata sono diritti fondamentali nell'era digitale. Sono anche diritti "abilitanti" che favoriscono e rafforzano la tutela di altri diritti fondamentali che possono essere pregiudicati dalla sorveglianza da parte dello Stato o di privati, quali la dignità umana, la libertà di espressione, la libertà di pensiero, di coscienza e di religione o la libertà di riunione, il diritto a un equo processo, a un ricorso effettivo o alla non discriminazione. Il regolamento generale sulla protezione dei dati, la direttiva relativa alla protezione dei dati nelle attività di polizia e giudiziarie e la direttiva relativa alla vita privata e alle comunicazioni elettroniche hanno messo l'Europa in prima linea nella protezione dei diritti fondamentali online. La crescente digitalizzazione in tutti i settori della vita pone sfide per la protezione dei dati e per la vita privata e familiare. Altre normative, come la legge sulla governance dei dati, su cui è stato raggiunto di recente un accordo politico tra i colegislatori, mirano a promuovere l'emergere di una forte economia dei dati, regolamentando i servizi di intermediazione dei dati, l'altruismo dei dati e il riutilizzo dei dati pubblici protetti, in linea e in conformità con il regime di protezione dei dati.

Che rapporto c'è tra il diritto al rispetto della vita privata e il diritto alla protezione dei dati?

Si tratta di diritti fondamentali distinti ma sovrapposti, sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali.

- Il rispetto della vita privata e familiare (privacy) protegge la sfera privata dalle intrusioni illecite. Ad esempio, in virtù di tale diritto la riservatezza delle comunicazioni interpersonali e i dispositivi elettronici degli utenti sono tutelati da intrusioni non autorizzate.

- La "protezione dei dati" si applica solo quando i dati personali sono trattati con mezzi automatizzati o in forma manuale strutturata. Il diritto non si limita alle informazioni relative alla sfera privata, ma riguarda tutti i dati personali di una persona, compresa la sua vita professionale. I principi fondamentali della protezione dei dati sono la trasparenza, l'equità e la legittimità delle attività di trattamento dei dati personali. Per protezione dei dati si intende inoltre che i dati personali dovrebbero essere trattati solo per finalità specifiche ed esplicite, dovrebbero essere esatti, limitati a quanto necessario e conservati in condizioni di sicurezza e solo per il tempo necessario.

Nella pratica, il solido quadro giuridico dell'UE è costantemente messo alla prova. Le organizzazioni dei consumatori e le OSC che si occupano di diritti fondamentali ne lamentano la mancata applicazione nei casi di violazione del GDPR[104]. Negli ultimi anni l'UE e gli Stati membri hanno adottato una serie di misure per tutelare la sicurezza pubblica e affrontare le sfide in materia di sicurezza avvalendosi della tecnologia moderna. In tale contesto le organizzazioni della società civile hanno espresso preoccupazione per la

[104] Ad esempio https://www.beuc.eu/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf e https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf.

proporzionalità delle politiche di sorveglianza e sicurezza, ad esempio per quanto riguarda il monitoraggio delle frontiere dell'UE[105] o nel caso di normative adottate o proposte che consentano alle autorità di esaminare le comunicazioni private a fini di sicurezza[106]. Anche la società civile e le organizzazioni del settore hanno espresso preoccupazione per quelli che percepiscono come tentativi da parte degli Stati membri di indebolire la crittografia[107].

Le autorità di protezione dei dati e gli organi giurisdizionali nazionali hanno garantito un ricorso effettivo in tutti i casi in cui le misure di sorveglianza adottate da soggetti pubblici e privati costituiscono una violazione dei diritti fondamentali. Di seguito alcuni esempi: i) la decisione dell'autorità svedese di protezione dei dati relativa all'uso di videocamere indossabili da parte dei controllori dei mezzi di trasporto pubblici di Stoccolma, in cui si criticava la mancanza di trasparenza e l'eccessiva raccolta di dati, imponendo una sanzione di 16,1 milioni di SEK[108]; ii) il *Conseil d'Etat* (Consiglio di Stato) francese ha deciso che la polizia doveva smettere di utilizzare droni per verificare il rispetto delle norme sul distanziamento interpersonale, in quanto tali droni avevano la capacità tecnica di identificare le persone e non erano utilizzati in conformità alla normativa in materia di protezione dei dati[109].

Il quadro europeo relativo a un'identità digitale proposto offrirà a tutti i cittadini e a tutti i residenti dell'UE, su base volontaria, un portafoglio digitale affidabile e sicuro sotto il totale controllo degli utenti in quanto elemento fondamentale "autosovrano" per garantire l'accesso ai servizi pubblici e privati digitali e condividendo una serie di attributi e credenziali[110].

8.1 Conservazione dei dati

Dal 2014 le leggi nazionali che prevedono la conservazione dei metadati delle telecomunicazioni (dati relativi al traffico e all'ubicazione) a fini di contrasto e intelligence sono state ritenute non conformi ai requisiti del diritto dell'UE dalla Corte di giustizia dell'Unione europea. La Corte ha ritenuto che tali leggi nazionali costituiscono un'ingerenza grave e sproporzionata nei diritti alla vita privata e alla protezione dei dati, in quanto i metadati delle comunicazioni possono rivelare informazioni su un numero significativo di aspetti della vita privata degli interessati[111]. Pur riconoscendo che le misure di conservazione dei dati perseguono obiettivi legittimi di interesse pubblico, la Corte ha spesso rilevato che,

[105] https://edri.org/our-work/technological-testing-grounds-border-tech-is-experimenting-with-peoples-lives/.
[106] Cfr. ad esempio https://edri.org/wp-content/uploads/2020/10/20201020-EDRi-Open-letter-CSAM-and-encryption-FINAL.pdf oppure https://netzpolitik.org/2021/finfisher-wir-verklagen-das-bka-auf-den-staatstrojaner-vertrag/.
[107] Cfr. ad esempio https://www.statewatch.org/news/2020/november/eu-council-set-to-adopt-declaration-against-encryption/ oppure https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/it/pdf?utm_source=dsms- oppure https://www.bitkom.org/sites/default/files/2020-12/201211_pp_bitkom_grundsatzerklarung-verschlusselung_0.pdf auto&utm_medium=email&utm_campaign=Encryption%3A+Council+adopts+resolution+on+security+through+encryption+and+security+despite+encryption.
[108] https://edpb.europa.eu/news/national-news/2021/unlawful-use-body-cams-stockholms-public-transport_it; https://www.imy.se/tillsyner/storstockholms-lokaltrafik-sl/.
[109] https://www.conseil-etat.fr/actualites/actualites/le-conseil-d-etat-ordonne-a-l-etat-de-cesser-immediatement-la-surveillance-par-drone-du-respect-des-regles-sanitaires.
[110] COM(2021) 281 final.
[111] Cfr. ad esempio la sentenza del 2 marzo 2021, Prokuratuur, causa C-746/18, ECLI:EU:C:2021:152.

fatte salve alcune eccezioni[112], il diritto dell'Unione osta a misure legislative che impongono ai prestatori di servizi di comunicazione elettronica, a titolo preventivo, un obbligo di conservazione generale e indiscriminata dei dati relativi al traffico e all'ubicazione. Nella **strategia dell'UE per la lotta alla criminalità organizzata 2021-2025** del 14 aprile 2021, la Commissione ha annunciato l'intenzione di analizzare e delineare possibili approcci alla conservazione dei dati, in linea con le sentenze della Corte, che rispondano alle esigenze delle autorità di contrasto e giudiziarie in un modo che sia operativamente utile, tecnicamente possibile e giuridicamente valido, anche nel pieno rispetto dei diritti fondamentali, e di consultare gli Stati membri entro la fine di giugno 2021 per definire il modo in cui procedere. La Commissione sta attualmente portando avanti un processo di consultazione ed esaminerà attentamente i risultati di tale consultazione prima di prendere una decisione sulla possibile via da seguire.

8.2 Cifratura

La cifratura è essenziale per tutelare i diritti fondamentali e proteggere i sistemi e le transazioni. La legislazione dell'UE prevede la cifratura come misura volta a garantire la tutela di diritti fondamentali quali la vita privata, la protezione dei dati personali[113] e la libertà di espressione, nonché a garantire la cibersicurezza[114]. Inoltre, la cifratura è importante anche per la protezione dei segreti aziendali e, di conseguenza, aiuta le persone a beneficiare del loro diritto di esercitare un'attività economica. Dall'inizio della pandemia di COVID-19, insieme al crescente ricorso agli strumenti digitali in tutti gli ambiti della vita, è aumentato il numero di attacchi informatici. Tali attacchi hanno causato gravi danni alle imprese e ai servizi essenziali, compresi i sistemi sanitari, e hanno compromesso i diritti delle persone, mettendo in evidenza l'importanza della cifratura per gli attori pubblici e privati in quanto tutela la riservatezza delle informazioni[115].

Tuttavia l'uso della cifratura consente anche ai criminali di celare la propria identità e nascondere il contenuto delle loro comunicazioni. A seguito degli inviti degli Stati membri, la Commissione si è impegnata a valutare soluzioni tecniche, operative e giuridiche equilibrate rispetto a tali sfide. Tali soluzioni devono mantenere l'efficacia della cifratura nel proteggere la vita privata e la sicurezza delle comunicazioni, fornendo nel contempo una risposta efficace alla criminalità e al terrorismo[116]. La Commissione intende suggerire nel 2022 un

[112] Cfr. la sentenza del 6 ottobre 2020, La Quadrature du Net e a., cause riunite C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791, nell'ambito della quale la Corte ha autorizzato la conservazione generalizzata dei dati relativi al traffico e all'ubicazione per evitare minacce gravi alla sicurezza nazionale, degli indirizzi IP attribuiti all'origine di una connessione per contrastare i reati gravi e dei dati relativi all'identità civile per contrastare la criminalità in generale.

[113] Articolo 32, paragrafo 1, lettera a), articolo 34, paragrafo 3, lettera a), articolo 6, paragrafo 4, lettera e), considerando 83 del regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE; considerando 60, articolo 31, paragrafo 3, lettera a), della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie; considerando 20 in combinato disposto con l'articolo 4 della direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche.

[114] Articolo 40, paragrafo 1, del codice europeo delle comunicazioni elettroniche e considerando 96; considerando 40 del regolamento (UE) 2019/881 (regolamento sulla cibersicurezza).

[115] Il comitato europeo per la protezione dei dati (EDPB) ha adottato i propri orientamenti 1/2021 relativi alla notifica delle violazioni dei dati (versione per la consultazione pubblica). La cifratura svolge un ruolo importante nella riduzione al minimo dei rischi di violazione dei dati personali.

[116] L'impegno rientra nella strategia dell'Unione della sicurezza di luglio 2020.

percorso da seguire per affrontare la questione dell'accesso legittimo e mirato alle informazioni cifrate nell'ambito delle indagini e delle azioni penali, che si baserà su una mappatura approfondita indicante le modalità di utilizzo della cifratura da parte degli Stati membri, unitamente a un processo di consultazione dei portatori di interessi per esaminare e valutare le opzioni concrete (giuridiche, etiche e tecniche)[117].

8.3 Identificazione biometrica remota

Le norme dell'UE in materia di protezione dei dati vietano in linea di principio il trattamento di dati biometrici allo scopo di identificare in modo univoco una persona fisica, salvo a determinate condizioni[118]. Il trattamento di tali dati deve avere una base giuridica fondata sulla legislazione in materia di protezione dei dati, che potrebbe essere costituita dal consenso liberamente prestato da tutti gli interessati, difficilmente ottenibile nella pratica, o in alternativa da una normativa dell'UE o di uno Stato membro che persegua un interesse pubblico rilevante, come la prevenzione della minaccia concreta e imminente di un attentato terroristico. Nell'ambito delle attività di contrasto, il trattamento sarà autorizzato ai sensi di legge. Nel caso in cui il trattamento dei dati biometrici si basi sulla legge, tale legge deve essere proporzionata all'obiettivo perseguito, rispettare l'essenza del diritto alla protezione dei dati e di altri diritti fondamentali e prevedere misure adeguate e specifiche per tutelare i diritti fondamentali e gli interessi degli interessati.

Le OSC hanno espresso preoccupazioni circa il crescente ricorso alle tecnologie di identificazione biometrica remota in diversi Stati membri e ne hanno chiesto il divieto[119]. L'uso di sistemi di identificazione biometrica remota è stato criticato anche dal Garante europeo della protezione dei dati, dal comitato europeo per la protezione dei dati, che comprende le autorità nazionali per la protezione dei dati[120], e da altri organismi nazionali per i diritti fondamentali, come il *Defenseur des Droits* in Francia[121]. In alcuni casi le autorità per la protezione dei dati sono intervenute per porre fine all'uso illecito di tale tecnologia, ad esempio in una scuola in Francia, da parte della polizia in Svezia o di un supermercato in Olanda[122].

[117] Strategia contro la criminalità organizzata, adottata il 14 aprile 2021.

[118] Cfr. l'articolo 9 del regolamento generale sulla protezione dei dati e articolo 10 della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie. Ai sensi del GDPR, tale trattamento può essere effettuato solo per un numero limitato di motivi, principalmente per motivi di interesse pubblico rilevante. In tal caso, il trattamento deve essere effettuato sulla base del diritto dell'Unione o degli Stati membri, rispettare il requisito di proporzionalità e l'essenza del diritto alla protezione dei dati e prevedere garanzie adeguate. A norma della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, tale trattamento deve essere strettamente necessario, autorizzato in linea di principio dal diritto dell'UE o degli Stati membri e soggetto a garanzie adeguate.

[119] https://edri.org/our-work/biometric-mass-surveillance-flourishes-in-germany-and-the-netherlands/ e https://reclaimyourface.eu/it/.

[120] https://edps.europa.eu/press-publications/press-news/press-releases/2021/edpb-edps-call-ban-use-ai-automated-recognition_en.

[121] https://www.defenseurdesdroits.fr/fr/communique-de-presse/2021/07/technologies-biometriques-la-defenseure-des-droits-appelle-au-respect.

[122] Autorità di protezione dei dati olandese: L'autorità di protezione dei dati olandese ha inviato una diffida formale a un supermercato per aver utilizzato la tecnologia di riconoscimento facciale | Comitato europeo per la protezione dei dati (europa.eu); sanzione dell'autorità di protezione dei dati svedese alla polizia per l'uso di Clearview: La Svezia sanziona la polizia per l'uso illecito della tecnologia di riconoscimento facciale - POLITICO Pro; autorità di protezione dei dati francese sull'uso del riconoscimento biometrico nelle scuole:

Oltre al quadro esistente, il regolamento sull'IA che la Commissione ha proposto ad aprile 2021 (cfr. il capitolo 4) vieta l'identificazione biometrica remota in tempo reale in spazi accessibili al pubblico mentre la autorizza a fini di attività di contrasto in tre limitate eccezioni e a condizione che si applichino garanzie specifiche[123].

8.4 Istruzione

Durante la pandemia di COVID-19 gli istituti di istruzione e formazione hanno utilizzato diverse piattaforme e strumenti online. Spesso considerato una "soluzione rapida", l'uso di soluzioni commerciali di apprendimento digitale e di software per monitorare gli studenti durante lo svolgimento degli esami a distanza ha suscitato preoccupazioni in merito alla possibilità che tali sistemi potessero sfruttare i dati degli utenti a fini di lucro, anziché per pratiche pedagogiche significative.

Il polo europeo per l'istruzione digitale, istituito nell'ambito del piano d'azione per l'istruzione digitale, consiste in un forum volto a elaborare misure per garantire una più stretta collaborazione intersettoriale, promuovere lo scambio tra educatori, sviluppare strumenti per la garanzia della qualità e garantire il rispetto della protezione dei dati e della vita privata. Tra questi, la garanzia della qualità e la fiducia svolgeranno un ruolo fondamentale: la prima al fine di promuovere una comprensione condivisa dei principali standard qualitativi per l'istruzione digitale; la seconda al fine di garantire il rispetto dei principi fondamentali in materia di utilizzo dei dati, etica e vita privata. Questi due elementi, oltre a rafforzare il livello di preparazione digitale degli istituti di istruzione e formazione europei, possono aumentare la cooperazione al fine di migliorare la qualità complessiva delle soluzioni digitali disponibili.

8.5 Salute

Molti aspetti della **risposta alla pandemia di COVID-19** comportano il trattamento di dati personali, compresi i dati sanitari, che a causa della loro sensibilità sono soggetti a ulteriori norme previste dal GDPR. Il trattamento dei dati personali deve essere limitato a quanto necessario e proporzionato per conseguire l'obiettivo e rispettare i requisiti del GDPR. L'approccio dell'UE si è basato su tale principio. Ad esempio, la Commissione ha fornito agli Stati membri orientamenti[124] sulle app a sostegno della lotta alla pandemia e ha supportato il loro lavoro su un pacchetto di strumenti contenente requisiti per le app[125] e specifiche tecniche per l'interoperabilità[126] tra le applicazioni nazionali di allerta nell'UE. La Commissione ha istituito un gateway per consentire l'invio di tali allerte a livello transfrontaliero e tra le diverse applicazioni dei vari Stati membri. La Commissione ha inoltre

---

Secondo il garante della privacy francese la sperimentazione del riconoscimento facciale nelle scuole superiori è illegale - POLITICO Pro.

[123] L'articolo 5, paragrafo 1, lettera d), della proposta stabilisce che tale uso deve essere strettamente necessario per i) la ricerca mirata di potenziali vittime specifiche di reato, compresi i minori scomparsi; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di un attacco terroristico; oppure iii) il rilevamento dell'autore o del sospettato di un reato contemplato dal mandato d'arresto europeo e la punizione nello Stato membro interessato per un periodo della durata massima di almeno tre anni. L'uso è inoltre soggetto all'autorizzazione di un organo giudiziario o di un altro organo indipendente e a limiti per quanto riguarda il tempo, la portata geografica e le banche dati ricercate.

[124] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52020XC0417(08).

[125] https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[126] https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.

proposto una piattaforma per lo scambio di dati dei moduli di localizzazione dei passeggeri[127] a sostegno del tracciamento transfrontaliero dei contatti in riferimento ai mezzi di trasporto. Come passo successivo, si è impegnata a proporre un quadro giuridico dell'UE per un approccio coordinato alla registrazione dello storico dei viaggi recenti nella misura necessaria ad arginare la diffusione della COVID-19, sulla base dell'esperienza dei moduli di localizzazione dei passeggeri.

Inoltre, il 14 giugno 2021 il Parlamento europeo e il Consiglio hanno adottato un regolamento che istituisce il sistema del certificato COVID digitale dell'UE per agevolare la libera circolazione durante la pandemia di COVID-19[128]. È stata istituita un'infrastruttura a sostegno del rilascio e della verifica dei certificati di vaccinazione, di test e di guarigione, al fine di semplificare il controllo delle misure di sanità pubblica durante i viaggi (ad esempio per le deroghe ai requisiti di quarantena). Per facilità d'uso, i certificati sono disponibili in formato sia digitale che cartaceo. In tutti i casi, le categorie di dati e il trattamento sono limitati a quanto necessario per la finalità in questione; ad esempio, a coloro che verificano i certificati è vietato conservare il loro contenuto a seguito della verifica. Inoltre il quadro di fiducia istituito per il certificato COVID digitale dell'UE garantisce che la verifica dei certificati possa essere eseguita offline, senza informare l'emittente o altri terzi in merito alla verifica. La trasparenza è sempre fondamentale, sia per garantire il rispetto della Carta e della legislazione applicabile, sia per creare fiducia e mantenerla. Il risultato mostra che, quando le misure sono concepite con attenzione, la protezione dei dati è coerente con l'attuazione di misure efficaci in materia di sanità pubblica e può contribuire a promuoverle e a garantire che il quadro dell'UE in materia di protezione dei dati offra la flessibilità richiesta.

La Commissione sta attualmente preparando una proposta legislativa sullo **spazio europeo dei dati sanitari**, che dovrebbe essere adottata all'inizio del 2022. Lo spazio europeo dei dati sanitari mira ad agevolare la fornitura di servizi sanitari digitali e a promuovere l'accesso ai dati sanitari per la ricerca, l'innovazione, l'elaborazione delle politiche e le attività normative, migliorando nel contempo il controllo dei dati personali da parte dei cittadini. L'iniziativa sullo spazio europeo dei dati sanitari sarà pienamente conforme alle norme dell'UE applicabili in materia di protezione dei dati.

8.6 Applicazione delle norme

Le autorità nazionali di controllo competenti per il monitoraggio e l'applicazione delle norme in materia di protezione dei dati e della vita privata sono il fondamento del sistema di governance per la protezione dei dati nell'UE. Tali autorità e gli organi giurisdizionali nazionali sono responsabili del monitoraggio e dell'applicazione delle norme previste dal GDPR, dalle leggi nazionali di recepimento della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie[129] e della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Per la Commissione, uno degli obiettivi principali è che gli Stati membri attuino tali norme in modo corretto ed efficace. In virtù del diritto dell'UE, gli Stati membri hanno l'obbligo di garantire l'indipendenza delle proprie autorità per la protezione dei

[127] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A02017D0253-20210726.
[128] https://eur-lex.europa.eu/eli/reg/2021/953/oj?locale=it, accompagnato da https://eur-lex.europa.eu/eli/reg/2021/954/oj?locale=it.
[129] https://eur-lex.europa.eu/eli/dir/2016/680/2016-05-04?locale=it.

dati e di assegnare loro risorse sufficienti per svolgere le attività di controllo[130]. La Commissione segue gli sviluppi riguardanti l'indipendenza, i compiti, i poteri e le risorse delle autorità di controllo e, in caso di inosservanza delle norme dell'UE da parte degli Stati membri, ricorre a procedure di infrazione per garantire che tali norme siano applicate in modo efficace.

Le autorità per la protezione dei dati collaborano in seno al comitato europeo per la protezione dei dati per garantire la coerenza nell'applicazione del GDPR, in particolare nei casi transfrontalieri. Dopo tre anni di applicazione del GDPR, l'efficacia di tale cooperazione è stata oggetto di critiche[131] e l'EDPB continuerà ad adoperarsi per aumentarne l'efficienza[132]. La Commissione condivide il parere del Consiglio[133], del Parlamento europeo e dell'EDPB[134] secondo cui occorre ora concentrarsi sul miglioramento dell'attuazione e sulle azioni volte a rafforzare l'applicazione della normativa dell'UE in materia di protezione dei dati.

8.7 Protezione dei dati personali al di fuori dell'UE

Un aspetto essenziale della tutela dei diritti fondamentali in un ambiente online consiste nel garantire la continuità della protezione delle persone quando i loro dati escono dall'UE. Poiché nell'odierno mondo interconnesso i dati personali si spostano facilmente a livello transfrontaliero e i flussi di dati sono diventati parte integrante del commercio, della cooperazione normativa e persino dell'interazione sociale, le tutele garantite dal regolamento generale sulla protezione dei dati e dalla direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie sarebbero inefficaci se si limitassero al trattamento all'interno dell'UE.

In tale contesto, la Commissione ha continuato a portare avanti il suo ambizioso programma volto a promuovere un elevato livello di protezione quando i dati degli europei sono trasferiti all'estero, agevolando nel contempo i flussi di dati. Fra l'altro ha partecipato attivamente al dialogo con i principali partner al fine di giungere a una "decisione di adeguatezza", che stabilisce che un paese terzo garantisce un livello di protezione dei dati "sostanzialmente equivalente" a quello assicurato nell'UE. Tale dialogo ha prodotto risultati importanti, quali l'adozione di due decisioni di adeguatezza per il Regno Unito (ai sensi del GDPR e della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie) e la conclusione di colloqui sull'adeguatezza con la Corea del Sud.

Inoltre, a seguito dell'annullamento da parte della Corte di giustizia della precedente decisione di adeguatezza dello scudo per la privacy, l'UE e gli Stati Uniti hanno intensificato i negoziati su un nuovo quadro UE-USA in materia di tutela della vita privata per i trasferimenti transatlantici di dati che garantisca il pieno rispetto della sentenza della Corte.

[130] Panoramica dell'EDPB sulle risorse messe a disposizione dagli Stati membri alle autorità per la protezione dei dati e sulle azioni di esecuzione delle autorità per la protezione dei dati del 5 agosto 2021, pubblicata l'11 agosto al seguente indirizzo: https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf.
[131] Cfr. ad esempio la risoluzione 2020/2717(RSP) del Parlamento europeo.
[132] Strategia dell'EDPB 2021-2023, adottata il 15 dicembre 2020, disponibile al seguente indirizzo: edpb_strategy2021-2023_it.pdf (europa.eu).
[133] Posizione e conclusioni del Consiglio in merito all'applicazione del regolamento generale sulla protezione dei dati (GDPR) - Adozione, 14994/1/19 REV 1, 19 dicembre 2019, disponibile al seguente indirizzo: pdf (europa.eu).
[134] Relazione annuale 2020 dell'EDPB, 2 giugno 2021, disponibile al seguente indirizzo: Relazione annuale 2020 dell'EDPB | Comitato europeo per la protezione dei dati (europa.eu).

Inoltre, a giugno 2020 la Commissione ha adottato clausole contrattuali tipo aggiornate per il trasferimento di dati personali verso paesi terzi, che riflettono nuovi requisiti a norma del GDPR e sono adeguate alle esigenze dell'economia digitale moderna. Si tratta di clausole tipo di protezione dei dati che un esportatore e un importatore di dati possono, su base volontaria, integrare nei loro accordi contrattuali (ad esempio un contratto di servizio che preveda il trasferimento di dati personali) e che dovrebbero assicurare adeguate garanzie in materia di protezione dei dati.

La Commissione continua inoltre a partecipare all'iniziativa *Data Free Flow with Trust* (libera circolazione dei dati con fiducia), lanciata dal Giappone nel 2019 e successivamente approvata dal G20 e dal G7. Un elemento centrale di questo concetto, attualmente all'esame dell'OCSE con la partecipazione attiva dell'UE e dei suoi Stati membri, consiste nel tracciare una linea di demarcazione tra l'accesso legittimo ai dati da parte delle pubbliche amministrazioni, con limitazioni e garanzie adeguate, e la sorveglianza abusiva da parte dello Stato.

9. Unire le forze per fare dell'era digitale un'opportunità per i diritti fondamentali

Considerando le sfide interconnesse e le misure corrispondenti esaminate nella presente relazione, è indubbio che l'UE e i suoi Stati membri sono impegnati nella tutela e nella promozione dei diritti fondamentali nell'era digitale e stanno collaborando per individuare le migliori pratiche per raggiungere tale scopo. Gli esempi menzionati nei capitoli precedenti sono solo alcune delle numerose opportunità per imparare gli uni dagli altri e plasmare in modo positivo i cambiamenti derivanti dalla transizione digitale.

La Commissione utilizza molti strumenti per garantire il rispetto dei diritti sanciti dalla Carta, sia nell'elaborazione delle sue iniziative legislative e politiche che nell'applicazione del diritto dell'UE. In particolare, la Commissione valuterà attentamente gli effetti sui diritti fondamentali e mirerà a bilanciare tali effetti nelle prossime iniziative della Commissione nel 2022, tra cui le proposte legislative circa:

- il diritto alla riparazione;
- la ciberresilienza;
- i servizi digitali per la mobilità;
- i pagamenti istantanei;
- l'accesso reciproco alle informazioni in materia di sicurezza per gli agenti di prima linea tra l'UE e i principali paesi terzi;
- una legge per la libertà dei media; e
- norme vincolanti riguardanti gli organismi per la parità.

Inoltre, nel contesto del decennio digitale, la Commissione proporrà di includere un insieme di principi digitali in una solenne dichiarazione interistituzionale tra la Commissione europea, il Parlamento europeo e il Consiglio. Tale dichiarazione informerà gli utenti e orienterà i responsabili politici e gli operatori digitali in merito al percorso europeo verso la trasformazione digitale.

La Commissione invita il Parlamento europeo, il Consiglio e gli Stati membri a utilizzare la presente relazione annuale sull'applicazione della Carta dei diritti fondamentali dell'Unione europea per avviare scambi sulle sfide e le opportunità per la tutela dei diritti fondamentali nell'era digitale. Accoglie con favore l'impegno del Consiglio a procedere a uno scambio di opinioni sulla base delle relazioni della Commissione[135] e accoglierebbe con favore anche una discussione in seno al Parlamento europeo. In particolare, tali scambi potrebbero contribuire ad affrontare al meglio le sfide future, nello specifico la lotta contro l'incitamento all'odio e la disinformazione, come garantire il bilanciamento dei poteri in relazione alle misure di sorveglianza e, più in generale, come applicare in modo efficace le leggi per tutelare i diritti fondamentali nell'ambiente digitale. Tali scambi possono contribuire a inquadrare gli sviluppi politici in modo costruttivo e proficuo.

Questi sforzi congiunti per rendere la Carta efficace nell'era digitale, unitamente al piano d'azione per la democrazia europea[136] e al meccanismo europeo per lo Stato di diritto[137], dimostrano l'impegno dell'UE a promuovere e proteggere i valori su cui si fonda.

[135] Conclusioni del Consiglio sul rafforzamento dell'applicazione della Carta dei diritti fondamentali dell'8 marzo 2021, paragrafo 26.
[136] Comunicazione della Commissione sul piano d'azione per la democrazia europea, COM(2020) 790.
[137] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/rule-law/rule-law-mechanism_it.