Consiglio dell'Unione europea

Bruxelles, 27 febbraio 2020
(OR. en)

6263/1/20
REV 1 (bg,cs,da,el,es,et,fi,hr,hu,it,lt,lv,mt,nl, pl,pt,ro,sk,sl,sv)

JAI 148
COPEN 59
CYBER 26
DATAPROTECT 22
EJUSTICE 21
COSI 27
IXIM 29
ENFOPOL 54
FREMP 14
TELECOM 23
RELEX 149
MI 48
COMPET 56

NOTA DI TRASMISSIONE

n. doc. Comm.:	COM(2020) 64 final
Oggetto:	RELAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO E AL COMITATO ECONOMICO E SOCIALE EUROPEO **Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità**

Si trasmette in allegato, per le delegazioni, una **nuova versione** del documento COM(2020) 64 final.

All.: COM(2020) 64 final

COMMISSIONE
EUROPEA

Bruxelles, 19.2.2020
COM(2020) 64 final

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

Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità

RELAZIONE SULLE IMPLICAZIONI DELL'INTELLIGENZA ARTIFICIALE, DELL'INTERNET DELLE COSE E DELLA ROBOTICA IN MATERIA DI SICUREZZA E DI RESPONSABILITÀ

1. Introduzione

L'intelligenza artificiale (IA)[1], l'Internet delle cose (IoT)[2] e la robotica creeranno nuove opportunità e apporteranno benefici alla nostra società. La Commissione, che ha riconosciuto l'importanza e il potenziale di queste tecnologie e la necessità di investimenti significativi nei relativi settori[3], è impegnata a fare dell'Europa un leader mondiale nel campo dell'intelligenza artificiale, dell'Internet delle cose e della robotica. Per conseguire questo obiettivo è necessario un quadro giuridico chiaro e prevedibile che affronti le sfide tecnologiche.

1.1. Il quadro vigente in materia di sicurezza e di responsabilità

L'obiettivo generale dei quadri giuridici in materia di sicurezza e di responsabilità è garantire che tutti i prodotti e servizi, compresi quelli che integrano le tecnologie digitali emergenti, funzionino in modo sicuro, affidabile e costante e che vi siano rimedi efficaci in caso di danni. Livelli elevati di sicurezza dei prodotti e dei sistemi che integrano le nuove tecnologie digitali e meccanismi solidi per rimediare ai danni verificatisi (ossia il quadro della responsabilità) contribuiscono a tutelare meglio i consumatori. Creano inoltre fiducia in queste tecnologie, che è un prerequisito per la loro adozione da parte di imprese e utilizzatori. Questa contribuirà, a sua volta, a rafforzare la competitività delle nostre imprese e a realizzare gli obiettivi dell'Unione[4]. Con l'emergere di nuove tecnologie, come l'intelligenza artificiale, l'Internet delle cose e la robotica, acquista particolare importanza un quadro chiaro in materia di sicurezza e di responsabilità, sia per tutelare i consumatori sia per garantire la certezza del diritto per le imprese.

L'Unione dispone di un quadro normativo solido e affidabile in materia di sicurezza e di responsabilità per danno da prodotti difettosi, oltre che di un solido corpus di norme di sicurezza, integrati dalla normativa nazionale non armonizzata in materia di responsabilità. Insieme, garantiscono il benessere dei cittadini nel mercato unico e incoraggiano l'innovazione e la diffusione delle tecnologie. Tuttavia, l'intelligenza artificiale, l'Internet delle cose e la robotica stanno trasformando le caratteristiche di molti prodotti e servizi.

Nella comunicazione dal titolo "L'intelligenza artificiale per l'Europa"[5], adottata il 25 aprile 2018, la Commissione ha annunciato la presentazione di una relazione per valutare le implicazioni delle nuove tecnologie digitali per i quadri vigenti in materia di sicurezza e responsabilità. La presente relazione delinea ed esamina le implicazioni maggiori per i quadri

---

1 La definizione di intelligenza artificiale del gruppo di esperti ad alto livello sull'intelligenza artificiale (AI HLEG) è disponibile all'indirizzo https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines.

2 La definizione di Internet delle cose contenuta nella raccomandazione ITU-T Y.2060 è disponibile all'indirizzo https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060.

3 SWD(2016) 110, COM(2017) 9, COM(2018) 237 e COM(2018) 795.

4 https://ec.europa.eu/growth/industry/policy_it.

5 https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM%3A2018%3A237%3AFIN.
Il documento di lavoro della Commissione che accompagna la relazione (SWD(2018) 137)(https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137) ha delineato un primo quadro delle sfide in termini di responsabilità poste dalle tecnologie digitali emergenti.

normativi in materia di responsabilità e sicurezza in relazione all'intelligenza artificiale, all'Internet delle cose e alla robotica, e ne individua le potenziali lacune. Gli orientamenti formulati nella presente relazione, che accompagna il libro bianco sull'intelligenza artificiale, sono forniti come contributo alla discussione e rientrano nella più ampia consultazione dei portatori di interessi. La sezione sulla sicurezza è basata sulla valutazione[6] della direttiva macchine[7] e sul lavoro con i pertinenti gruppi di esperti[8]. La sezione sulla responsabilità si basa sulla valutazione[9] della direttiva sulla responsabilità per danno da prodotti difettosi[10], sul contributo dei pertinenti gruppi di esperti[11] e sui contatti con i portatori di interesse. La presente relazione, che non mira a fornire un quadro completo delle norme vigenti in materia di sicurezza e responsabilità, si concentra sugli aspetti chiave finora individuati.

1.2. Caratteristiche delle tecnologie dell'intelligenza artificiale, dell'Internet delle cose e della robotica

L'intelligenza artificiale, l'Internet delle cose e la robotica hanno molte caratteristiche in comune. Consentono di combinare **connettività**, **autonomia** e **dipendenza dai dati** per svolgere compiti con un livello minimo o nullo di controllo o supervisione umani. I sistemi dotati di intelligenza artificiale possono inoltre migliorare le proprie prestazioni apprendendo dall'esperienza. La loro **complessità** si riflette sia nella pluralità degli operatori economici partecipanti alla **catena di approvvigionamento** che nella molteplicità di componenti, parti, software, sistemi o servizi, che insieme formano i nuovi ecosistemi tecnologici. A ciò si aggiunge l'**apertura** agli aggiornamenti e ai miglioramenti dopo l'immissione sul mercato. La grande quantità di dati necessari, la dipendenza da algoritmi e l'**opacità** del processo decisionale dell'intelligenza artificiale rendono più difficile prevedere il comportamento dei prodotti basati sull'intelligenza artificiale e comprendere le possibili cause di un danno. Infine, la connettività e l'apertura possono anche esporre i prodotti basati sull'intelligenza artificiale e sull'Internet delle cose a **minacce informatiche**.

---

6 SWD(2018) 161 final.

7 Direttiva 2006/42/CE.

8 La rete per la sicurezza dei consumatori, istituita dalla direttiva 2001/95/CE relativa alla sicurezza generale dei prodotti, e i gruppi di esperti istituiti a norma della direttiva 2006/42/CE relativa alle macchine e della direttiva 2014/53/UE sulle apparecchiature radio, composti di rappresentanti degli Stati membri, delle imprese e di altri portatori di interessi, quali le associazioni dei consumatori.

9 COM(2018) 246 final.

10 Direttiva 85/374/CEE.

11 Il gruppo di esperti sulla responsabilità e le nuove tecnologie è stato istituito con il compito di fornire consulenza alla Commissione in merito all'applicabilità della direttiva sulla responsabilità per danno da prodotti difettosi e delle norme nazionali in materia di responsabilità civile e di sostenerla nell'elaborazione di orientamenti per possibili adeguamenti della normativa applicabile in relazione alle nuove tecnologie. È costituito da due formazioni: la "formazione sulla responsabilità per danno da prodotti difettosi" e la "formazione sulle nuove tecnologie", cfr. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1.
Per la relazione presentata dalla "formazione sulle nuove tecnologie" dal titolo "*Liability for Artificial Intelligence and other emerging digital technologies*" (responsabilità per l'intelligenza artificiale e altre tecnologie digitali emergenti), cfr. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

1.3. Opportunità create dall'intelligenza artificiale, dall'Internet delle cose e dalla robotica

Accrescere la fiducia degli utilizzatori e l'accettazione sociale delle tecnologie emergenti, migliorare i prodotti, i processi e i modelli di business e aiutare i produttori europei a diventare più efficienti: sono solo alcune delle opportunità offerte dall'intelligenza artificiale, dall'Internet delle cose e dalla robotica.

Oltre agli incrementi di produttività e di efficienza, l'intelligenza artificiale promette anche di consentire agli esseri umani di sviluppare livelli di intelligenza non ancora raggiunti, che apriranno la strada a nuove scoperte e contribuiranno a risolvere alcune delle più grandi sfide dell'umanità: dal trattamento delle malattie croniche, alla previsione dell'insorgenza di malattie, alla riduzione del numero delle vittime di incidenti stradali, alla lotta ai cambiamenti climatici o all'anticipazione delle minacce alla cibersicurezza.

Queste tecnologie possono generare molti benefici, migliorando la sicurezza dei prodotti, rendendoli meno esposti a determinati rischi. Ad esempio, i veicoli connessi e automatizzati potrebbero migliorare la sicurezza stradale, dato che la maggior parte degli incidenti stradali è attualmente causata da errore umano[12]. Inoltre, i sistemi dell'Internet delle cose sono progettati per ricevere ed elaborare grandi quantità di dati provenienti da fonti diverse. Questa maggiore mole di informazioni potrebbe essere utilizzata per consentire ai prodotti di autoadattarsi e diventare quindi più sicuri. Le nuove tecnologie possono contribuire ad accrescere l'efficacia dei richiami dei prodotti, ad esempio, grazie al fatto che i prodotti stessi potrebbero avvertire gli utilizzatori e prevenire così problemi di sicurezza[13]. Se utilizzando un prodotto connesso dovesse sorgere un problema di sicurezza, i produttori potrebbero comunicare direttamente con gli utilizzatori, sia per avvertirli dei rischi che per risolvere direttamente il problema fornendo, ad esempio, un aggiornamento di sicurezza. Ad esempio, in occasione del richiamo di uno dei suoi dispositivi nel 2017, un produttore di smartphone ha effettuato un aggiornamento del software per ridurre a zero la capacità della batteria dei telefoni richiamati[14], in modo da impedire agli utilizzatori di continuare a utilizzare i dispositivi pericolosi.

Le nuove tecnologie possono inoltre contribuire a migliorare la tracciabilità dei prodotti. Ad esempio, le caratteristiche di connettività dell'Internet delle cose possono consentire alle imprese e alle autorità di vigilanza del mercato di tracciare i prodotti pericolosi e di individuare i rischi nella catene di approvvigionamento[15].

Tuttavia, oltre a offrire opportunità all'economia e alla società, l'intelligenza artificiale, l'Internet delle cose e la robotica possono anche creare un rischio di pregiudizio di interessi

---

[12] Secondo le stime, circa il 90 % degli incidenti stradali è causato da errore umano. Cfr. la relazione della Commissione dal titolo "Salvare vite umane: migliorare la sicurezza dei veicoli nell'UE" (COM(2016) 0787 final).

[13] Ad esempio, il conducente di un'autovettura può essere invitato a rallentare nel caso si sia verificato un incidente più avanti.

[14] OCSE (2018), "*Measuring and maximising the impact of product recalls globally: OECD workshop report*"(misurare e massimizzare l'impatto dei richiami di prodotti a livello internazionale: relazione informativa dell'OCSE), *OECD Science, Technology and Industry Policy Papers*, No. 56, OECD Publishing, Parigi, https://doi.org/10.1787/ab757416-en.

[15] OCSE (2018), "*Enhancing product recall effectiveness globally: OECD background report*" (migliorare l'efficienza dei richiami di prodotti a livello internazionale: relazione informativa dell'OCSE) *OECD Science, Technology and Industry Policy Papers*, No. 58, OECD Publishing, Parigi, https://doi.org/10.1787/ef71935c-en.

giuridicamente protetti, sia materiali che immateriali. Tale rischio di pregiudizio aumenta con l'ampliarsi del campo delle applicazioni. A tale riguardo, è essenziale analizzare se e in che misura il vigente quadro giuridico in materia di sicurezza e responsabilità sia ancora idoneo a proteggere gli utilizzatori.

2. Sicurezza

Nella comunicazione della Commissione dal titolo "Creare fiducia nell'intelligenza artificiale antropocentrica" si legge: "***I sistemi di IA dovrebbero inoltre contenere meccanismi di sicurezza fin dalla progettazione, per garantire che siano sicuri in modo verificabile in ogni fase****, considerando soprattutto la* ***sicurezza fisica e mentale*** *di tutte le persone coinvolte.*"[16]

La presente sezione analizza la normativa dell'Unione in materia di sicurezza dei prodotti per valutare se il vigente quadro normativo dell'Unione contenga gli elementi idonei per garantire che le tecnologie emergenti, in particolare i sistemi di intelligenza artificiale, integrino gli aspetti della sicurezza e della *security* sin dalla progettazione.

La presente relazione esamina principalmente la direttiva relativa alla sicurezza generale dei prodotti[17] e la normativa armonizzata in materia di prodotti che segue le norme orizzontali del "nuovo approccio"[18] e/o del "nuovo quadro normativo" (di seguito "normativa o quadro dell'Unione in materia di sicurezza dei prodotti")[19]. Le norme orizzontali garantiscono la coerenza tra le norme settoriali sulla sicurezza dei prodotti.

La normativa dell'Unione in materia di sicurezza dei prodotti mira a garantire che i prodotti immessi sul mercato dell'Unione soddisfino requisiti elevati in materia di salute, sicurezza e ambiente e che tali prodotti possano circolare liberamente in tutta l'Unione. La normativa settoriale[20] è integrata dalla direttiva sulla sicurezza generale dei prodotti[21], che prescrive che tutti i prodotti di consumo, anche se non disciplinati dalla normativa settoriale dell'Unione, devono essere sicuri. Le norme sulla sicurezza sono integrate dalla vigilanza del mercato e dai poteri conferiti alle autorità nazionali nel quadro del regolamento sulla vigilanza del mercato[22] e della direttiva sulla sicurezza generale dei prodotti[23]. Nel settore dei trasporti

---

16 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Creare fiducia nell'intelligenza artificiale antropocentrica (COM(2019) 168 final dell'8.4.2019).

17 Direttiva 2001/95/CE del Parlamento europeo e del Consiglio, del 3 dicembre 2001, relativa alla sicurezza generale dei prodotti (GU L 11 del 15.1.2002, pag. 4).

18 GU C 136 del 4.6.1985, pag. 1.

19 Regolamento (CE) n. 765/2008 e decisione n. 768/2008/CE.

20 Tale quadro non include la normativa dell'Unione in materia di trasporti e di automobili.

21 Direttiva 2001/95/CE del Parlamento europeo e del Consiglio, del 3 dicembre 2001, relativa alla sicurezza generale dei prodotti (GU L 11 del 15.1.2002, pag. 4).

22 Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30), https://eur-lex.europa.eu/eli/reg/2008/765/oj, e, a decorrere dal 2021, regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011 (GU L 169 del 25.6.2019, pag. 1), http://data.europa.eu/eli/reg/2019/1020/oj.

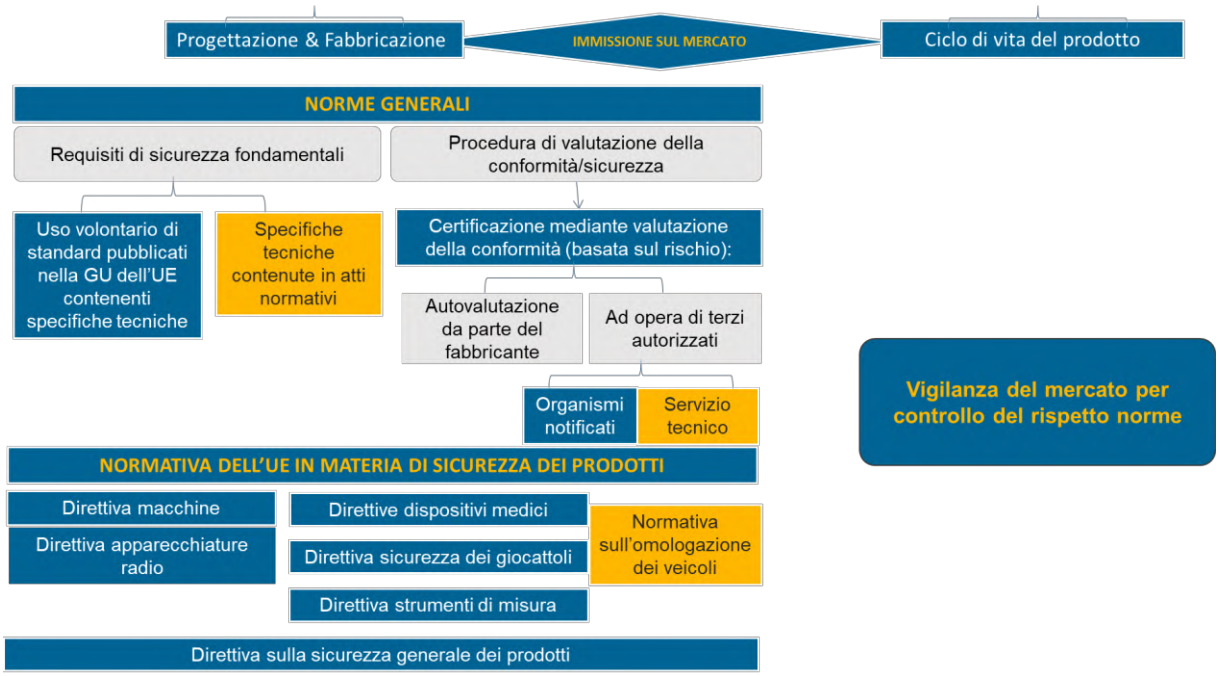
23 Articolo 8, paragrafo 1, lettera b), e paragrafo 3, della direttiva sulla sicurezza generale dei prodotti.

vigono ulteriori norme nazionali e dell'Unione per la messa in servizio di veicoli a motore[24], aeromobili e navi e norme chiare in materia di sicurezza di funzionamento, che prevedono compiti per gli operatori e compiti di vigilanza per le autorità.

La standardizzazione europea è anch'essa un elemento essenziale della normativa dell'Unione in materia di sicurezza dei prodotti. Data la dimensione mondiale della digitalizzazione e delle tecnologie digitali emergenti, la cooperazione internazionale in materia di standardizzazione assume particolare importanza per la competitività dell'industria europea.

Buona parte del quadro normativo dell'Unione in materia di sicurezza dei prodotti è stato scritto prima dell'emergere delle tecnologie digitali, come l'intelligenza artificiale, l'Internet delle cose o la robotica. Pertanto, non sempre esso contiene disposizioni che trattano esplicitamente le nuove sfide e i nuovi rischi posti dalle tecnologie emergenti. Tuttavia, sebbene il quadro vigente in materia di sicurezza dei prodotti sia neutro sotto il profilo tecnologico, ciò non significa che non si applichi ai prodotti che incorporano dette tecnologie. Inoltre, gli atti normativi successivi che compongono detto quadro normativo, ad esempio nel settore dei dispositivi medici o degli autoveicoli, prendono già esplicitamente in considerazione alcuni aspetti legati all'emergere delle tecnologie digitali, ad esempio le decisioni automatizzate, il software come prodotto a sé stante e la connettività.

La logica alla base della vigente normativa dell'Unione in materia di sicurezza dei prodotti[25]



Le sfide che le tecnologie digitali emergenti rappresentano per il quadro normativo dell'Unione in materia di sicurezza dei prodotti sono illustrate qui di seguito.

---

[24] Ad esempio, la direttiva 2007/46/CE sull'omologazione dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, componenti ed entità tecniche destinati a tali veicoli, e il regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio, del 30 maggio 2018, relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche indipendenti destinati a tali veicoli, che modifica i regolamenti (CE) n. 715/2007 e (CE) n. 595/2009 e abroga la direttiva 2007/46/CE.

[25] Questo quadro non comprende le disposizioni della normativa sul ciclo di vita dei prodotti, ossia gli aspetti relativi all'utilizzo e alla manutenzione, e viene presentato solo a fini illustrativi.

La **connettività** è una caratteristica fondamentale di un numero sempre crescente di prodotti e servizi. Questa caratteristica mette in discussione il concetto tradizionale di sicurezza, dato che la connettività può compromettere la sicurezza del prodotto sia direttamente sia indirettamente, in caso di attacco informatico che rappresenti una minaccia alla *security* e crei un pregiudizio per la sicurezza degli utilizzatori.

Si può citare ad esempio la segnalazione al sistema di allarme rapido dell'UE inviata dall'Islanda riguardante un orologio intelligente per bambini[26]. Pur non causando direttamente un danno ai bambini, il prodotto non garantisce un livello minimo di *security* e può pertanto essere utilizzato come strumento per avere accesso ai bambini. Una delle funzioni previste del prodotto è garantire la sicurezza dei bambini grazie alla localizzazione; pertanto, il consumatore si aspetterebbe che il prodotto non comporti minacce alla *security* per i bambini, in quanto questi potrebbero essere localizzati e/o contattati da estranei, con il pregiudizio che ne deriverebbe per la loro sicurezza.

Un altro esempio è illustrato da una segnalazione della Germania riguardante un'autovettura[27]. La radio del veicolo può presentare lacune nella *security* del software che consentono l'accesso non autorizzato da parte di terzi ai sistemi di controllo interconnessi del veicolo. Se dette lacune fossero sfruttate da terzi per scopi dolosi, potrebbe verificarsi un incidente stradale.

Le applicazioni industriali possono anch'esse essere esposte a minacce informatiche che mettono a rischio la sicurezza delle persone su più ampia scala, quando tali applicazioni non presentano i livelli di *security* necessari. Si pensi ad esempio all'attacco informatico al sistema di controllo critico di un impianto industriale allo scopo di innescare un'esplosione che potrebbe causare vittime.

Di norma, la normativa dell'Unione in materia di sicurezza dei prodotti non prevede specifici requisiti obbligatori contro le minacce informatiche che incidono sulla sicurezza degli utilizzatori. Tuttavia, disposizioni in materia di *security* sono previste dal regolamento sui dispositivi medici[28], dalla direttiva sugli strumenti di misura[29], dalla direttiva sulle apparecchiature radio[30] e dalla normativa sull'omologazione dei veicoli[31]. Il regolamento sulla cibersicurezza[32] istituisce quadri volontari di certificazione della cibersicurezza per i prodotti, i servizi e i processi delle tecnologie dell'informazione e della comunicazione (TIC), mentre la pertinente normativa dell'Unione sulla sicurezza dei prodotti stabilisce requisiti obbligatori.

Inoltre, anche il rischio di perdita della connettività delle tecnologie digitali emergenti può comportare rischi per l'incolumità. Ad esempio, se un allarme antincendio collegato perde la connettività, potrebbe non avvertire l'utilizzatore in caso di incendio.

---

[26] Segnalazione RAPEX dell'Islanda pubblicata sul sito web del Safety Gate dell'UE (A12/0157/19).

[27] Segnalazione RAPEX della Germania pubblicata sul sito web del Safety Gate dell'UE (A12/1671/15).

[28] Regolamento (UE) 2017/745 relativo ai dispositivi medici.

[29] Direttiva 2014/32/UE relativa alla messa a disposizione sul mercato di strumenti di misura.

[30] Direttiva 2014/53/UE sulle apparecchiature radio.

[31] Direttiva 2007/46/CE concernente l'omologazione dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, componenti ed entità tecniche destinati a tali veicoli. A decorrere dal 1° settembre 2020 la direttiva sarà abrogata e sostituita dal regolamento (UE) 2018/858 relativo all'omologazione dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche indipendenti destinati a tali veicoli, che modifica i regolamenti (CE) n. 715/2007 e (CE) n. 595/2009 e abroga la direttiva 2007/46/CE.

[32] Regolamento (UE) 2019/881.

Nella vigente normativa dell'Unione in materia di sicurezza dei prodotti la sicurezza è considerata un obiettivo di politica pubblica. Il concetto di sicurezza è legato all'uso del prodotto e ai rischi, ad esempio meccanici, elettrici, ecc., che devono essere affrontati per garantire la sicurezza del prodotto. Va osservato che, a seconda dell'atto normativo dell'Unione in materia di sicurezza dei prodotti, l'uso del prodotto comprende non solo l'uso previsto ma anche l'uso prevedibile e in alcuni casi, come nella direttiva macchine[33], anche l'uso scorretto ragionevolmente prevedibile.

Il concetto di sicurezza nell'attuale normativa dell'Unione in materia di sicurezza dei prodotti è in linea con il concetto esteso di sicurezza al fine di proteggere i consumatori e gli utilizzatori. Pertanto, il concetto di sicurezza dei prodotti include la protezione contro tutti i tipi di rischi derivanti dal prodotto, non solo i rischi meccanici, chimici o elettrici ma anche i rischi informatici e i rischi connessi alla perdita di connettività dei dispositivi.

Al riguardo si potrebbero introdurre disposizioni esplicite per quanto riguarda l'ambito di applicazione dei pertinenti atti normativi dell'Unione, al fine di garantire una migliore protezione degli utilizzatori e una maggiore certezza del diritto.

L'**autonomia**[34] è una delle caratteristiche principali dell'intelligenza artificiale. Gli esiti non intenzionali dell'intelligenza artificiale potrebbero danneggiare gli utilizzatori e le persone esposte.

Nella misura in cui il "comportamento" futuro dei prodotti basati sull'intelligenza artificiale può essere determinato in anticipo mediante la valutazione del rischio effettuata dal fabbricante prima dell'immissione sul mercato, il quadro dell'Unione in materia di sicurezza dei prodotti fissa già l'obbligo per i produttori di tener conto, nella valutazione dei rischi, dell'"uso"[35] dei prodotti per tutto il loro ciclo di vita. Stabilisce inoltre che i fabbricanti devono fornire agli utilizzatori istruzioni e informazioni sulla sicurezza o avvertenze[36]. Ad esempio, al riguardo la direttiva sulle apparecchiature radio[37] impone al fabbricante di inserire istruzioni sulle modalità di utilizzo delle apparecchiature radio in base all'uso previsto.

In futuro si potranno anche creare situazioni in cui gli esiti dei sistemi di intelligenza artificiale non potranno essere determinati pienamente in anticipo. In tali situazioni la valutazione del rischio effettuata prima dell'immissione del prodotto sul mercato può non riflettere più l'uso, il funzionamento o il comportamento del prodotto. In questi casi, nella

---

33 Direttiva 2006/42/CE relativa alle macchine.

34 Sebbene i prodotti basati sull'intelligenza artificiale possano agire in modo autonomo, percependo l'ambiente circostante e senza seguire istruzioni predefinite, il loro comportamento è limitato dagli scopi loro attribuiti e da altre scelte di progettazione compiute dagli sviluppatori.

35 Secondo la normativa dell'Unione in materia di sicurezza dei prodotti, i produttori devono effettuare la valutazione dei rischi sulla base dell'uso previsto del prodotto, dell'uso prevedibile e/o dell'uso scorretto ragionevolmente prevedibile.

36 Decisione n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e che abroga la decisione 93/465/CEE (GU L 218 del 13.8.2008, pag. 82). L'allegato I, articolo R2, paragrafo 7, recita: "*I fabbricanti garantiscono che il prodotto sia accompagnato da istruzioni e informazioni sulla sicurezza in una lingua che può essere facilmente compresa dai consumatori e dagli altri utenti finali, secondo quanto determinato dallo Stato membro interessato.*"

37 Articolo 10, paragrafo 8, relativo alle istruzioni per l'utilizzatore finale, e allegato VI, che si riferisce alla dichiarazione di conformità UE.

misura in cui l'uso previsto, inizialmente progettato dal fabbricante, è modificato[38] a causa del comportamento autonomo e venga meno la conformità ai requisiti di sicurezza, si potrebbe prevedere l'obbligo di una nuova valutazione del prodotto capace di autoapprendimento[39].

A norma del quadro vigente, quando vengono a conoscenza del fatto che un prodotto, durante tutto il suo ciclo di vita, presenta rischi aventi un impatto sulla sicurezza, i produttori sono già tenuti a informare immediatamente le autorità competenti e ad adottare provvedimenti per prevenire i rischi per gli utilizzatori[40].

Oltre alla valutazione del rischio effettuata prima dell'immissione sul mercato del prodotto, potrebbe essere introdotta un'ulteriore procedura di valutazione del rischio, da effettuarsi nel caso in cui il prodotto subisse importanti modifiche durante il ciclo di vita, ad esempio una funzione diversa, non prevista dal fabbricante nella valutazione iniziale del rischio. Detta valutazione dovrebbe riguardare l'impatto sulla sicurezza dovuto al comportamento autonomo durante l'intero ciclo di vita del prodotto. La valutazione del rischio dovrebbe essere effettuata dall'operatore economico appropriato. I pertinenti atti normativi dell'Unione potrebbero inoltre includere obblighi rafforzati per i fabbricanti in materia di istruzioni e avvertenze per gli utilizzatori.

Una simile valutazione del rischio è già obbligatoria nella normativa in materia di trasporti[41]; ad esempio, nel trasporto ferroviario, la normativa prevede che, in caso di modifica di un veicolo ferroviario dopo che quest'ultimo è stato certificato, il soggetto che introduce la modifica deve seguire una procedura specifica e attenersi a criteri chiari e definiti per determinare se occorra rivolgersi alle autorità.

La caratteristica dell'autoapprendimento dei prodotti e sistemi di intelligenza artificiale può consentire alla macchina di prendere decisioni che si discostano da quanto inizialmente previsto dai fabbricanti e, pertanto, dalle aspettative degli utilizzatori. Questo elemento solleva interrogativi in merito al controllo umano, in quanto gli esseri umani dovrebbero poter scegliere se e come delegare le decisioni ai prodotti e ai sistemi di intelligenza

---

[38] Finora l'espressione "capace di autoapprendimento" è stata utilizzata nell'ambito dell'intelligenza artificiale per lo più per indicare che le macchine sono in grado di apprendere durante l'addestramento; non è ancora un requisito che le macchine dotate di intelligenza artificiale continuino ad apprendere anche dopo la loro messa in funzione; al contrario, in particolare nel settore della salute, le macchine dotate di intelligenza artificiale cessano normalmente di apprendere dopo che il loro addestramento si è concluso con successo. Pertanto, per il momento il comportamento autonomo dei sistemi di intelligenza artificiale non implica che il prodotto svolge compiti non previsti dagli sviluppatori.

[39] Il che è in linea con la sezione 2.1 della "guida blu all'attuazione della normativa UE sui prodotti, 2016".

[40] Articolo 5 della direttiva 2001/95/CE del Parlamento europeo e del Consiglio, del 3 dicembre 2001, relativa alla sicurezza generale dei prodotti.

[41] La procedura da seguire in caso di modifiche del sistema ferroviario che possono avere un impatto sulla sicurezza (ad esempio, modifiche tecniche, operative o anche organizzative che potrebbero incidere sul processo operativo o di manutenzione) è descritta nell'allegato I del regolamento di esecuzione (UE) 2015/1136 (GU L 185 del 14.7.2015, pag. 6).
In caso di "modifica rilevante", un "organismo di valutazione" indipendente (che può essere l'autorità nazionale preposta alla sicurezza o un terzo tecnicamente competente) dovrebbe fornire al proponente il rapporto di valutazione della sicurezza.
A seguito della procedura di analisi del rischio, il proponente applicherà le misure appropriate per attenuare i rischi (se il proponente è un'impresa ferroviaria o il gestore dell'infrastruttura, l'applicazione del regolamento è un compito che rientra nel suo sistema di gestione della sicurezza, la cui applicazione a sua volta è sottoposta alla supervisione dell'autorità nazionale preposta alla sicurezza).

artificiale, per realizzare gli scopi che si sono prefissi[42]. La vigente normativa dell'Unione in materia di sicurezza dei prodotti non affronta esplicitamente la questione della sorveglianza umana dei prodotti e dei sistemi dell'intelligenza artificiale capaci di autoapprendimento[43].

I pertinenti atti normativi dell'Unione potrebbero prevedere, come misura di salvaguardia, obblighi specifici in materia di sorveglianza umana, sin dalla progettazione e per tutto il ciclo di vita dei prodotti e dei sistemi di intelligenza artificiale.

Il "comportamento" futuro delle applicazioni di intelligenza artificiale potrebbe generare **rischi per la salute mentale**[44] degli utilizzatori, dovuti, ad esempio, alla collaborazione con robot e sistemi di intelligenza artificiale umanoidi, nel contesto domestico o di lavoro. A tale riguardo, oggigiorno il concetto di sicurezza è utilizzato di norma per riferirsi alla minaccia, percepita dall'utilizzatore, di danni fisici che potrebbero derivare dalla tecnologia digitale emergente. Allo stesso tempo il quadro giuridico dell'Unione definisce i prodotti sicuri come prodotti che non presentano alcun rischio o solo rischi minimi per la sicurezza e la salute delle persone. È comunemente riconosciuto che la definizione di salute comprende sia il benessere fisico che quello mentale. Tuttavia, i rischi per la salute mentale dovrebbero essere esplicitamente ricompresi dalla nozione di sicurezza del prodotto nel quadro normativo.

Ad esempio, l'autonomia non dovrebbe causare stress e disagi eccessivi per lunghi periodi né nuocere alla salute mentale. A tale riguardo, i fattori che influiscono positivamente sulla sensazione di sicurezza degli anziani[45] sono: avere relazioni sicure con il personale sanitario, avere il controllo delle routine quotidiane e esserne informati. I produttori di robot che interagiscono con gli anziani dovrebbero tenere conto di questi fattori per prevenire i rischi per la salute mentale.

Nella pertinente normativa dell'Unione si potrebbero introdurre obblighi espliciti, anche a carico dei produttori di robot umanoidi dotati di intelligenza artificiale, di tener conto esplicitamente dei danni immateriali che i loro prodotti potrebbero causare agli utilizzatori, in particolare agli utilizzatori vulnerabili come le persone anziane in contesti di cura.

Un'altra caratteristica essenziale dei prodotti e dei sistemi basati sull'intelligenza artificiale è la **dipendenza dai dati**. L'accuratezza e la pertinenza dei dati sono essenziali per garantire che i sistemi e i prodotti basati sull'intelligenza artificiale prendano decisioni secondo quanto previsto dal produttore.

La normativa dell'Unione in materia di sicurezza dei prodotti non disciplina esplicitamente i rischi per la sicurezza derivanti da dati errati. Tuttavia, nelle fasi di progettazione e di prova i produttori dovrebbero anticipare, sulla base dell'"uso" del prodotto, l'accuratezza dei dati e la loro pertinenza per le funzioni di sicurezza.

---

[42] *Policy and investment recommendations for trustworthy artificial intelligence* (raccomandazioni sulle politiche e gli investimenti per un'intelligenza artificiale affidabile), gruppo di esperti ad alto livello sull'intelligenza artificiale, giugno 2019.

[43] Ciò non esclude tuttavia che la sorveglianza possa essere necessaria in determinate situazioni, in ragione di alcuni obblighi più generali vigenti in materia di immissione sul mercato del prodotto.

[44] Secondo la costituzione dell'OMS, primo trattino, la salute è uno stato di totale benessere fisico, mentale e sociale e non semplicemente l'assenza di malattia o infermità (https://www.who.int/about/who-we-are/constitution). (https://www.who.int/about/who-we-are/constitution)

[45] *Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction* (robot sociali: aspetti tecnologici, sociali ed etici dell'interazione tra umani e robot), pagg. 237-264, Neziha Akalin, Annica Kristoff ersson e Amy Loutfi, luglio 2019.

Ad esempio, un sistema basato sull'intelligenza artificiale progettato per il rilevamento di specifici oggetti può avere difficoltà a riconoscere gli oggetti in condizioni di scarsa illuminazione; pertanto i progettisti dovrebbero includere dati provenienti da prove del prodotto sia in ambienti normalmente illuminati che in ambienti poco illuminati.

Un altro esempio riguarda i robot agricoli, ad esempio i robot per la raccolta della frutta, che sono progettati per reperire e localizzare i frutti maturi sugli alberi o a terra. Sebbene gli algoritmi già in uso registrino tassi di successo nella classificazione di oltre il 90 %, una carenza nella serie di dati che alimenta gli algoritmi può indurre i robot a prendere decisioni sbagliate e, di conseguenza, a causare danni ad animali o persone.

Occorre pertanto chiedersi se la normativa dell'Unione in materia di sicurezza dei prodotti debba contenere disposizioni specifiche riguardanti i rischi per la sicurezza derivanti da dati errati nella fase della progettazione e i meccanismi per garantire che la qualità dei dati sia mantenuta per tutto il periodo di uso dei prodotti e dei sistemi di intelligenza artificiale.

L'**opacità** è un'altra caratteristica saliente di alcuni dei prodotti e sistemi basati sull'intelligenza artificiale, che può derivare dalla loro capacità di migliorare le prestazioni grazie all'esperienza acquisita. A seconda dell'approccio metodologico, i prodotti e i sistemi basati sull'intelligenza artificiale possono essere caratterizzati da vari livelli di opacità. Può essere pertanto difficile ricostruire il processo decisionale del sistema ("effetto scatola nera"). Non è necessario che gli esseri umani comprendano ogni singola fase del processo decisionale, ma dato che gli algoritmi di intelligenza artificiale sono sempre più avanzati e sono utilizzati in settori critici, è fondamentale che gli esseri umani possano capire come il sistema ha preso le decisioni algoritmiche. Questo aspetto è particolarmente importante per il meccanismo ex post di controllo del rispetto delle norme, in quanto consente alle autorità preposte di risalire alla responsabilità dei comportamenti e delle scelte dei sistemi di intelligenza artificiale. È quanto è stato riconosciuto anche dalla Commissione nella comunicazione dal titolo "Creare fiducia nell'intelligenza artificiale antropocentrica"[46].

La normativa dell'Unione in materia di sicurezza dei prodotti non affronta esplicitamente i crescenti rischi derivanti dall'opacità dei sistemi basati su algoritmi. È pertanto necessario prevedere requisiti di trasparenza degli algoritmi, nonché di solidità, responsabilità e, se del caso, di sorveglianza umana e di risultati non distorti[47], particolarmente importanti per il meccanismo ex post di controllo del rispetto della normativa e per rafforzare la fiducia nell'utilizzo di tali tecnologie. A tal fine si potrebbe imporre agli sviluppatori degli algoritmi l'obbligo di comunicare i parametri di progettazione e i metadati delle serie di dati in caso di incidente.

Altri rischi che possono incidere sulla sicurezza sono quelli dovuti alla **complessità dei prodotti e dei sistemi**, data la possibilità di integrare componenti, dispositivi e prodotti diversi, che possono influenzarsi reciprocamente nel loro funzionamento (ad esempio i prodotti che fanno parte di un ecosistema domotico).

Tale complessità è già affrontata dal quadro giuridico dell'Unione in materia di sicurezza indicato all'inizio della presente sezione[48]. In particolare, quando effettua la valutazione del

[46] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top

[47] Sulla base dei principali requisiti proposti dal gruppo di esperti ad alto livello negli orientamenti etici per un'IA affidabile: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines.

[48] Regolamento (CE) n. 765/2008, decisione n. 768/2008/CE e normativa settoriale armonizzata in materia di sicurezza dei prodotti, ad esempio la direttiva 2006/42/CE relativa alle macchine.

rischio del prodotto, il produttore deve tener conto dell'uso previsto, dell'uso prevedibile e, se del caso, dell'uso scorretto ragionevolmente prevedibile.

Al riguardo, **se prevede che il dispositivo sarà interconnesso e interagirà con altri dispositivi, il produttore deve tenerne conto nella valutazione del rischio**. L'uso o gli usi impropri sono determinati sulla base, ad esempio, della passata esperienza di uso dello stesso tipo di prodotto, delle inchieste sugli incidenti o del comportamento umano.

La complessità dei sistemi è affrontata in modo più specifico anche dalla normativa settoriale sulla sicurezza, come il regolamento sui dispositivi medici, e, in certa misura, nella normativa sulla sicurezza generale dei prodotti[49]. Ad esempio, il produttore di un dispositivo connesso, destinato a far parte di un ecosistema domotico, dovrebbe poter ragionevolmente prevedere che i suoi prodotti avranno un impatto sulla sicurezza di altri prodotti.

Inoltre, la normativa in materia di trasporti affronta tale complessità a livello di sistema. Per automobili, treni e aerei, l'omologazione e la certificazione sono effettuate sia per ogni componente che per l'intero veicolo o aeromobile. L'idoneità alla circolazione su strada, l'aeronavigabilità e l'interoperabilità ferroviaria sono oggetto della valutazione di sicurezza. Nei trasporti, i "sistemi" devono essere "autorizzati" da un'autorità, sulla base della valutazione di conformità a chiari requisiti tecnici rilasciata da un terzo, o dopo la dimostrazione di come i rischi sono affrontati. Di norma la soluzione risulta da una combinazione tra il livello "prodotto" e il livello "sistema".

La normativa dell'Unione in materia di sicurezza dei prodotti, compresa la normativa in materia di trasporti, tiene già conto in certa misura della complessità dei prodotti o dei sistemi per affrontare i rischi che possono avere un impatto sulla sicurezza degli utilizzatori.

I sistemi complessi spesso ricorrono a **software**, che è un componente essenziale dei sistemi basati sull'intelligenza artificiale. Di norma, nell'ambito della valutazione iniziale del rischio, il fabbricante del prodotto finale ha l'obbligo di prevedere i rischi del software integrato nel prodotto al momento dell'immissione sul mercato.

Alcuni atti normativi dell'Unione in materia di sicurezza dei prodotti si riferiscono esplicitamente al software integrato nel prodotto. Ad esempio, la direttiva macchine[50] impone di evitare che un'avaria del software del sistema di comando crei situazioni pericolose.

Nella normativa dell'Unione in materia di sicurezza dei prodotti, gli aggiornamenti del software potrebbero essere assimilati a interventi di manutenzione per motivi di sicurezza, purché non modifichino in misura significativa il prodotto già immesso sul mercato e non introducano nuovi rischi non previsti nella valutazione del rischio iniziale. Tuttavia, se l'aggiornamento del software modifica in misura sostanziale il prodotto in cui viene scaricato, l'intero prodotto potrebbe essere considerato un nuovo prodotto e la conformità alla pertinente normativa in materia di sicurezza dei prodotti deve essere rivalutata al momento della modifica[51].

Per il software indipendente, immesso sul mercato senza altri componenti o caricato dopo che il prodotto è stato immesso sul mercato, la normativa settoriale armonizzata dell'Unione in materia di sicurezza dei prodotti non contiene disposizioni specifiche. Tuttavia, alcuni atti

[49] L' articolo 2 della direttiva sulla sicurezza generale dei prodotti specifica che un prodotto sicuro tiene conto "*dell'effetto del prodotto su altri prodotti, qualora sia ragionevolmente prevedibile l'utilizzazione del primo con i secondi*".

[50] Allegato I, sezione 1.2.1, della direttiva macchine.

[51] La guida blu all'attuazione della normativa UE sui prodotti, 2016.

normativi dell'Unione disciplinano il software indipendente, ad esempio il regolamento sui dispositivi medici. Inoltre, il software indipendente caricato su prodotti connessi che comunicano tramite determinati moduli radio[52] può essere disciplinato anche dalla direttiva sulle apparecchiature radio, mediante atti delegati. Quest'ultima direttiva prevede che alcune specifiche classi o categorie di apparecchiature radio supportino caratteristiche che garantiscano che non sia compromessa la conformità delle apparecchiature quando viene caricato software[53].

Mentre la normativa dell'Unione sulla sicurezza dei prodotti tiene conto dei rischi per la sicurezza derivanti dal software integrato nel prodotto al momento dell'immissione sul mercato e dai possibili successivi aggiornamenti previsti dal fabbricante, per il software indipendente (ad esempio, un'applicazione da scaricare) potrebbero essere necessari requisiti specifici e/o espliciti. Particolare attenzione merita il software indipendente che garantisce le funzioni di sicurezza dei prodotti e dei sistemi di intelligenza artificiale.

Potrebbe essere necessario prevedere a carico dei fabbricanti l'ulteriore obbligo di garantire caratteristiche che impediscano il caricamento di software avente un impatto sulla sicurezza durante il ciclo di vita dei prodotti basati sull'intelligenza artificiale.

Infine, le tecnologie digitali emergenti presentano **catene di valore complesse**. Eppure, tale complessità non è una novità, né riguarda esclusivamente le nuove tecnologie digitali emergenti, come l'intelligenza artificiale o l'Internet delle cose. Si pensi, ad esempio, a prodotti quali computer, robot di servizio o sistemi di trasporto.

A norma del quadro dell'Unione in materia di sicurezza dei prodotti, a prescindere dalla complessità della catena del valore, la responsabilità della sicurezza del prodotto rimane a carico del produttore che immette il prodotto sul mercato. I produttori sono responsabili della sicurezza del prodotto finale, comprese le parti incorporate nel prodotto, ad esempio il software di un computer.

Alcuni atti normativi dell'Unione in materia di sicurezza dei prodotti contengono già disposizioni che fanno esplicito riferimento a situazioni in cui vari operatori economici intervengono su un determinato prodotto prima dell'immissione sul mercato. Ad esempio, la direttiva sugli ascensori[54] impone all'operatore economico responsabile della progettazione e della fabbricazione dell'ascensore di fornire alla persona responsabile dell'installazione[55] "*tutti i documenti e le informazioni necessari affinché quest'ultima possa garantire che l'ascensore venga installato e sottoposto a prova correttamente e in sicurezza.*" La direttiva macchine impone ai fabbricanti di apparecchiature di fornire all'operatore informazioni su come montare l'apparecchiatura con un'altra macchina[56].

---

[52] I moduli radio sono dispositivi elettronici che trasmettono e/o ricevono segnali radio (WIFI, Bluetooth) tra due dispositivi.

[53] Articolo 3, paragrafo 3, lettera i), della direttiva sulle apparecchiature radio.

[54] A norma dell'articolo 16, paragrafo 2, della direttiva 2014/33/UE.

[55] Nella direttiva 2014/33/UE relativa agli ascensori, l'installatore è l'equivalente del fabbricante e deve assumersi la responsabilità della progettazione, della fabbricazione, dell'installazione e dell'immissione sul mercato dell'ascensore.

[56] Direttiva macchine, allegato I, punto 1.7.4.2: "*Ciascun manuale di istruzioni deve contenere, se del caso, almeno le informazioni seguenti* [...] *i) le istruzioni per il montaggio, l'installazione e il collegamento, inclusi i disegni e i diagrammi e i sistemi di fissaggio e la designazione del telaio o dell'installazione su cui la macchina deve essere montata;*"

La normativa dell'Unione in materia di sicurezza dei prodotti tiene conto della complessità delle catene di valore, imponendo obblighi a diversi operatori economici secondo il principio della "responsabilità condivisa".

Sebbene la responsabilità del produttore per la sicurezza del prodotto finale si sia rivelata adeguata per le complesse catene di valore attuali, disposizioni esplicite che impongano specificamente la cooperazione tra gli operatori economici nella catena di approvvigionamento e gli utilizzatori potrebbero creare certezza giuridica in catene di valore forse ancora più complesse. In particolare, ogni partecipante alla catena di valore avente un impatto sulla sicurezza del prodotto (ad esempio i produttori di software) e sugli utilizzatori (ad esempio, se modifica il prodotto) si assumerebbe la propria responsabilità e fornirebbe al partecipante successivo nella catena le informazioni e le misure necessarie.

3. Responsabilità

A livello dell'Unione, le disposizioni in materia di sicurezza dei prodotti e di responsabilità per danno da prodotti difettosi sono due meccanismi complementari per perseguire lo stesso obiettivo di un mercato unico dei beni pienamente funzionante che garantisca elevati livelli di sicurezza, vale a dire che riduca al minimo il rischio di danni per gli utilizzatori e preveda il risarcimento dei danni dovuti a beni difettosi.

A livello nazionale, quadri non armonizzati in materia di responsabilità civile integrano le norme dell'Unione garantendo il risarcimento dei danni aventi origini diverse (prodotti e servizi) e contemplando vari soggetti responsabili (proprietari, operatori o fornitori di servizi).

Sebbene l'ottimizzazione delle norme dell'Unione in materia di sicurezza per l'intelligenza artificiale possa contribuire a evitare incidenti, questi possono comunque verificarsi. In tal caso interviene la responsabilità civile. Le norme in materia di responsabilità civile hanno una duplice funzione nella nostra società: da una parte, garantiscono che quanti hanno subito un danno causato da altri ottengano il risarcimento e, dall'altra, creano un incentivo economico per spingere la parte responsabile a evitare di causare il danno. Le norme in materia di responsabilità devono sempre trovare un equilibrio, tutelando i cittadini dai danni e consentendo allo stesso tempo alle imprese di innovare.

I quadri dell'Unione in materia di responsabilità hanno funzionato bene. Sono basati sull'applicazione parallela della direttiva sulla responsabilità per danno da prodotti difettosi (direttiva 85/374/CEE), che ha armonizzato la responsabilità del produttore di prodotti difettosi, e di altri regimi nazionali non armonizzati in materia di responsabilità.

La direttiva sulla responsabilità per danno da prodotti difettosi fornisce un livello di protezione che la sola responsabilità per colpa prevista a livello nazionale non è in grado di fornire. Introduce un regime di responsabilità oggettiva del produttore per i danni causati dai difetti del prodotto. In caso di danno fisico o materiale, la parte lesa ha diritto al risarcimento se prova il danno, il difetto del prodotto (ossia se dimostra che il prodotto non ha garantito la sicurezza che il pubblico ha il diritto di aspettarsi) e il nesso di causalità tra il prodotto difettoso e il danno.

In materia di responsabilità per colpa i regimi nazionali non armonizzati prevedono norme secondo le quali, per ottenere il risarcimento, il danneggiato deve dimostrare la colpa della persona responsabile, il danno e il nesso di causalità tra la colpa e il danno. I regimi nazionali prevedono anche regimi di responsabilità oggettiva in base ai quali il legislatore nazionale ha

attribuito la responsabilità del rischio ad un determinato soggetto, senza che il danneggiato debba provare la colpa/il difetto o il nesso di causalità tra la colpa/il difetto e il danno.

I regimi nazionali in materia di responsabilità offrono alle persone che hanno subito danni causati da prodotti e servizi la possibilità di presentare diverse domande parallele di risarcimento, sulla base della responsabilità per colpa o della responsabilità oggettiva. Spesso le domande di risarcimento sono rivolte contro soggetti responsabili diversi e sono soggette a condizioni diverse.

Ad esempio, di norma la vittima di un incidente automobilistico può far valere la responsabilità civile oggettiva nei confronti del proprietario del veicolo (ossia la persona che ha sottoscritto l'assicurazione di responsabilità civile autoveicoli) e la responsabilità per colpa nei confronti del conducente, entrambe sulla base delle norme di diritto civile nazionale, ma può anche chiedere il risarcimento nei confronti del fabbricante, in forza della direttiva sulla responsabilità per danno da prodotti difettosi, se l'autovettura presentava un difetto.

Conformemente alle norme armonizzate in materia di assicurazione dei veicoli a motore, l'uso del veicolo deve essere assicurato[57] e in pratica è all'assicuratore che ci si rivolge sempre in primis per il risarcimento per lesioni personali o danni materiali. Secondo dette norme, l'assicurazione obbligatoria risarcisce la vittima e tutela l'assicurato che, ai sensi del diritto civile nazionale[58], è tenuto al pagamento del risarcimento pecuniario per l'incidente in cui è coinvolto il veicolo. A norma della direttiva sulla responsabilità per danno da prodotti difettosi i produttori non sono soggetti all'obbligo di assicurazione. Nella normativa dell'Unione i veicoli autonomi non sono trattati diversamente dai veicoli non autonomi per quanto riguarda l'assicurazione autoveicoli. Come tutti i veicoli, anche questi ultimi devono essere coperti dall'assicurazione di responsabilità civile autoveicoli, che consente al danneggiato di ottenere il risarcimento nel modo più semplice.

La sottoscrizione di un'idonea assicurazione può attenuare le conseguenze negative degli incidenti consentendo il regolare risarcimento del danneggiato. Le norme chiare in materia di responsabilità aiutano le imprese di assicurazione a calcolare i rischi e a rivalersi sulla parte responsabile in ultima istanza del danno. Ad esempio, se un incidente stradale è causato da un difetto, l'assicuratore dell'autoveicolo può rivalersi sul fabbricante dopo aver risarcito la vittima.

Tuttavia, le caratteristiche delle tecnologie digitali emergenti, come l'intelligenza artificiale, l'Internet delle cose e la robotica, mettono alla prova taluni aspetti dei quadri normativi dell'Unione e nazionali in materia di responsabilità e potrebbero ridurne l'efficacia. Alcune di queste caratteristiche potrebbero rendere difficile risalire dal danno subito al comportamento umano, che giustificherebbe la domanda di risarcimento sulla base della responsabilità per colpa ai sensi delle norme nazionali. Di conseguenza, potrebbe essere difficile o costoso far valere le domande di risarcimento basate sulle norme nazionali in materia di responsabilità civile e pertanto le vittime potrebbero non essere adeguatamente risarcite. È importante che il livello di protezione delle vittime di incidenti causati da prodotti e servizi che integrano le tecnologie digitali emergenti, come l'intelligenza artificiale, non sia inferiore rispetto a quello concesso per altri prodotti e servizi simili, per i quali otterrebbero il risarcimento ai sensi del

[57] Armonizzata, per gli autoveicoli, dalla direttiva 2009/103/CE concernente l'assicurazione della responsabilità civile risultante dalla circolazione di autoveicoli e il controllo dell'obbligo di assicurare tale responsabilità.

[58] Nella maggior parte degli Stati membri vige la responsabilità oggettiva del soggetto in nome del quale il veicolo a motore è stato immatricolato.

diritto nazionale in materia di responsabilità civile. Ciò potrebbe ridurre l'accettazione sociale delle tecnologie emergenti e generare esitazione a usarle.

Sarà necessario valutare se le sfide poste dalle nuove tecnologie ai vigenti quadri normativi possano anche causare incertezza giuridica in merito al modo in cui sarebbero applicate le leggi vigenti (ad esempio, in che modo la nozione di colpa si applicherebbe ai danni causati dall'intelligenza artificiale). Questo potrebbe a sua volta scoraggiare gli investimenti e aumentare i costi di informazione e di assicurazione per i produttori e altre imprese della catena di approvvigionamento, in particolare le PMI europee. Inoltre, qualora alla fine gli Stati membri decidessero di affrontare le sfide per i quadri normativi nazionali in materia di responsabilità, si arriverebbe ad un'ulteriore frammentazione, che aumenterebbe i costi dell'introduzione di soluzioni di intelligenza artificiale innovative e ridurrebbe gli scambi transfrontalieri nel mercato unico. È importante che le imprese conoscano i rischi in termini di responsabilità lungo tutta la catena del valore e possano ridurli o prevenirli e assicurarsi efficacemente contro di essi.

Questo capitolo illustra in che modo le nuove tecnologie mettono alla prova i quadri normativi vigenti e come può essere affrontato tale problema. Inoltre, le specificità di alcuni settori, ad esempio il settore dell'assistenza sanitaria, meriterebbero ulteriori considerazioni.

Complessità dei prodotti, dei servizi e della catena di valore: negli ultimi decenni la tecnologia e l'industria hanno registrato un'evoluzione significativa. In particolare, la linea di separazione tra prodotti e servizi può non essere più così netta come una volta. I prodotti e i servizi sono sempre più interconnessi. I prodotti e le catene di valore complessi non sono una novità per l'industria europea o per il suo modello regolamentare, ma il software e l'intelligenza artificiale meritano un'attenzione particolare sotto il profilo della responsabilità per danno da prodotti difettosi. Il software è essenziale per il funzionamento di un gran numero di prodotti e può comprometterne la sicurezza. È integrato nei prodotti, ma può anche essere fornito separatamente per fare in modo che il prodotto possa essere usato come previsto. Né i computer né gli smartphone sarebbero di grande utilità senza il software. Il software può pertanto rendere difettoso un prodotto tangibile e causare danni fisici (cfr. il riquadro sul software nella sezione relativa alla sicurezza), di cui alla fine potrebbe essere ritenuto responsabile il fabbricante del prodotto ai sensi della direttiva sulla responsabilità per danno da prodotti difettosi.

Tuttavia, dato che il software può essere di molti tipi e forme, la classificazione del software come servizio o come prodotto potrebbe non sempre risultare semplice. Pertanto, mentre il software che consente il funzionamento di un prodotto tangibile potrebbe essere considerato parte o componente del prodotto, alcune forme di software indipendente potrebbero essere più difficili da classificare.

Nonostante l'ampiezza della definizione di prodotto fornita dalla direttiva sulla responsabilità per danno da prodotti difettosi, il suo ambito di applicazione andrebbe ulteriormente chiarito per rispecchiare meglio la complessità delle tecnologie emergenti e garantire che il risarcimento sia sempre possibile per i danni causati da prodotti difettosi a causa del software o di altre caratteristiche digitali. Si consentirebbe in tal modo agli operatori economici, quali gli sviluppatori di software, di valutare se possono essere considerati produttori ai sensi della direttiva sulla responsabilità per danno da prodotti difettosi.

Le applicazioni dell'intelligenza artificiale sono spesso integrate nei **complessi ambienti dell'Internet delle cose**, nei quali sono connessi e interagiscono tra loro molti dispositivi e servizi diversi. La combinazione di componenti digitali diversi in un ecosistema complesso e la pluralità di soggetti coinvolti possono rendere difficile accertare l'origine di un potenziale

danno e il soggetto responsabile dello stesso. A causa della complessità di queste tecnologie, può essere molto difficile per le vittime identificare il responsabile e dimostrare tutte le condizioni necessarie per il buon esito della domanda di risarcimento, come previsto dal diritto nazionale. I costi della consulenza in materia possono essere economicamente proibitivi e scoraggiare le vittime dal presentare domanda di risarcimento.

Inoltre, i prodotti e i servizi che dipendono dall'intelligenza artificiale interagiranno con le tecnologie tradizionali, accrescendo ulteriormente la complessità, anche per quanto riguarda la responsabilità. Ad esempio, per un certo periodo gli autoveicoli autonomi condivideranno la strada con gli autoveicoli tradizionali. Analoga complessità di interazione tra soggetti si creerà in alcuni settori dei servizi (come la gestione del traffico e l'assistenza sanitaria), in cui sistemi di intelligenza artificiale parzialmente automatizzati faranno da supporto al processo decisionale umano.

Secondo la relazione[59] della formazione sulle nuove tecnologie del gruppo di esperti sulla responsabilità e sulle nuove tecnologie, si potrebbero prevedere adeguamenti delle leggi nazionali per agevolare l'onere della prova per le vittime di danni dovuti all'intelligenza artificiale. Ad esempio, l'onere della prova potrebbe essere collegato al rispetto (da parte dell'operatore interessato) di specifici obblighi in materia di cibersicurezza o di altri obblighi di sicurezza stabiliti dalla legge: in caso di mancato rispetto di tali obblighi, potrebbe applicarsi una modifica dell'onere della prova per quanto riguarda la colpa e il nesso di causalità.

La Commissione sollecita osservazioni e commenti sulla necessità di e sulla misura in cui possa essere necessario attenuare le conseguenze della complessità alleggerendo/invertendo l'onere della prova imposto dalle norme nazionali in materia di responsabilità per i danni causati dal funzionamento delle applicazioni dell'intelligenza artificiale mediante un'opportuna iniziativa dell'UE.

Per quanto riguarda la normativa dell'Unione, secondo la direttiva sulla responsabilità per danno da prodotti difettosi, i prodotti che non soddisfano le norme di sicurezza obbligatorie sono considerati difettosi, indipendentemente dalla colpa del produttore. Tuttavia, vi potrebbero essere anche motivi per considerare modalità per alleggerire l'onere della prova a carico delle vittime nel quadro della direttiva: la direttiva si basa sulle norme nazionali relative alle prove e all'accertamento del nesso di causalità.

Connettività e apertura: attualmente non è del tutto chiaro quali possano essere le aspettative di sicurezza per quanto riguarda i danni derivanti dalle violazioni della cibersicurezza del prodotto e se questi danni sarebbero adeguatamente risarciti a norma della direttiva sulla responsabilità per danno da prodotti difettosi.

Le debolezze della cibersicurezza possono esistere fin dall'inizio, al momento della messa in circolazione del prodotto, ma possono anche sorgere in seguito, ben dopo l'immissione sul mercato.

Nel quadro dei regimi della responsabilità per colpa, la previsione di obblighi chiari in materia di cibersicurezza consente agli operatori di decidere cosa fare per evitare le conseguenze della responsabilità.

[59] *Liability for Artificial Intelligence and other emerging technologies* (responsabilità per l'intelligenza artificiale e altre tecnologie emergenti), relazione https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

Nel quadro della direttiva sulla responsabilità per danno da prodotti difettosi, può assumere maggiore importanza la questione di sapere se un produttore avrebbe potuto prevedere talune modifiche, tenendo conto dell'uso ragionevolmente prevedibile del prodotto. Ad esempio, si potrebbe assistere ad un aumento del ricorso alla "difesa basata sul difetto successivo", in base alla quale il produttore non è responsabile se il difetto non esisteva al momento in cui il prodotto è stato messo in circolazione o alla "difesa basata sui rischi di sviluppo" se le migliori conoscenze del momento non consentivano di prevedere il difetto. Inoltre, la responsabilità potrebbe essere ridotta nel caso in cui il danneggiato non proceda ai necessari aggiornamenti di sicurezza. Tale omissione potrebbe essere considerata concorso di colpa del danneggiato e pertanto ridurrebbe la responsabilità del produttore. Con l'aumento della prevalenza della nozione di utilizzo ragionevolmente prevedibile e delle questioni relative al concorso di colpa, come l'omesso scaricamento dell'aggiornamento di sicurezza, i danneggiati potrebbero avere difficoltà a ottenere il risarcimento dei danni causati da un difetto del prodotto.

Autonomia e opacità: le applicazioni dell'intelligenza artificiale sono in grado di agire autonomamente e possono svolgere un compito senza bisogno che ogni singolo passo sia predefinito e con un livello immediato di controllo o supervisione umani minimo o nullo. Può essere difficile, se non impossibile, capire gli algoritmi basati sull'apprendimento automatico (il cosiddetto "effetto scatola nera").

In aggiunta alla complessità discussa in precedenza, a causa dell'effetto scatola nera, in alcuni casi potrebbe essere difficile ottenere il risarcimento per i danni causati dalle applicazioni autonome dell'intelligenza artificiale. La necessità di comprendere l'algoritmo e i dati utilizzati dall'intelligenza artificiale richiede capacità analitiche e competenze tecniche che potrebbero avere un costo proibitivo per le vittime. Inoltre, l'accesso all'algoritmo e ai dati potrebbe risultare impossibile senza la collaborazione del potenziale soggetto responsabile. Pertanto, nella pratica le vittime potrebbero non essere in grado di far valere il diritto al risarcimento. Inoltre, non è chiaro in che modo si possa dimostrare la colpa di un'intelligenza artificiale che agisce autonomamente, né in che cosa potrebbe consistere la colpa della persona che utilizza l'intelligenza artificiale.

Le legislazioni nazionali hanno già sviluppato una serie di soluzioni per ridurre l'onere della prova a carico delle vittime in simili situazioni.

Nella normativa dell'Unione in materia di sicurezza dei prodotti e di responsabilità per danno da prodotti difettosi il principio guida è che spetta ai produttori garantire che tutti i prodotti immessi sul mercato siano sicuri, lungo tutto il ciclo di vita e per l'uso del prodotto ragionevolmente prevedibile. Ciò significa che il fabbricante dovrebbe garantire che il prodotto che utilizza l'intelligenza artificiale rispetti determinati parametri di sicurezza. Le caratteristiche dell'intelligenza artificiale non precludono il diritto a pretendere che i prodotti siano sicuri, che si tratti di tosaerba automatici o di robot chirurgici.

L'autonomia può incidere sulla sicurezza del prodotto, perché può alterarne in modo sostanziale le caratteristiche, comprese le caratteristiche di sicurezza. Si tratta di sapere a quali condizioni le caratteristiche di autoapprendimento prolungano la responsabilità del produttore e in quale misura il produttore dovrebbe essere in grado di prevedere alcune modifiche.

In stretto coordinamento con le corrispondenti modifiche del quadro normativo dell'Unione in materia di sicurezza, potrebbe essere rivista la nozione di "messa in circolazione" attualmente utilizzata dalla direttiva sulla responsabilità per danno da prodotti difettosi per tener conto del fatto che i prodotti possono cambiare e subire modifiche. Ciò potrebbe anche contribuire a chiarire chi è responsabile delle eventuali modifiche apportate al prodotto.

Secondo la relazione[60] della formazione sulle nuove tecnologie del gruppo di esperti sulla responsabilità e sulle nuove tecnologie, il funzionamento di alcuni dispositivi e servizi autonomi basati sull'intelligenza artificiale potrebbe avere un profilo di rischio specifico in termini di responsabilità, in quanto detti dispositivi e servizi possono causare danni significativi a importanti interessi giuridicamente rilevanti, quali la vita, la salute e la proprietà, ed esporre a rischi il pubblico in generale. Ciò potrebbe riguardare principalmente i dispositivi dotati di intelligenza artificiale che circolano negli spazi pubblici (ad esempio veicoli completamente autonomi, droni[61] e robot per la consegna di pacchi) o servizi basati sull'intelligenza artificiale che presentano rischi analoghi (ad esempio, i servizi di gestione del traffico che guidano o controllano veicoli o di gestione della distribuzione dell'energia elettrica). Le sfide che l'autonomia e l'opacità rappresentano per le norme nazionali in materia di responsabilità civile potrebbero essere affrontate seguendo un approccio basato sul rischio. I regimi di responsabilità oggettiva potrebbero garantire che, ogni volta che il rischio si concretizza, la vittima sia risarcita indipendentemente dalla colpa. L'impatto che la scelta del soggetto cui attribuire la responsabilità oggettiva di dette operazione può avere sullo sviluppo e sulla diffusione dell'intelligenza artificiale dovrebbe essere valutato con attenzione e si dovrebbe prevedere un approccio basato sul rischio.

Per il funzionamento delle applicazioni dell'intelligenza artificiale con un profilo di rischio specifico, la Commissione sollecita osservazioni e commenti sulla necessità di e sulla misura in cui possa essere necessaria la responsabilità oggettiva, quale prevista dalle legislazioni nazionali per rischi analoghi ai quali è esposto il pubblico (ad esempio per il funzionamento di veicoli a motore, aerei o centrali nucleari), per consentire il risarcimento efficace delle possibili vittime. La Commissione sollecita inoltre osservazioni e commenti sulla necessità di abbinare alla responsabilità oggettiva l'eventuale obbligo di sottoscrivere un'assicurazione disponibile, seguendo l'esempio della direttiva sull'assicurazione auto, al fine di garantire il risarcimento indipendentemente dalla solvibilità del responsabile e di contribuire a ridurre i costi dei danni.

Per il funzionamento di tutte le altre applicazioni dell'intelligenza artificiale, vale a dire la stragrande maggioranza delle applicazioni, la Commissione sta valutando la necessità di adeguare l'onere della prova del nesso di causalità e della colpa. A tale riguardo, la relazione[62] della formazione sulle nuove tecnologie del gruppo di esperti sulla responsabilità e sulle nuove tecnologie segnala tra l'altro le situazioni in cui la parte potenzialmente

[60] *Liability for Artificial Intelligence and other emerging technologies* (responsabilità per l'intelligenza artificiale e altre tecnologie emergenti), relazione https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

[61] Cfr. il "sistema di aeromobili senza equipaggio" di cui al regolamento di esecuzione (UE) 2019/947 della Commissione, del 24 maggio 2019, relativo alle norme e procedure applicabili all'esercizio di aeromobili senza equipaggio.

[62] *Liability for Artificial Intelligence and other emerging technologies* (responsabilità per l'intelligenza artificiale e altre tecnologie emergenti), relazione https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

responsabile non abbia registrato i dati pertinenti per valutare la responsabilità o non sia disposta a condividerli con la vittima.

4. Conclusioni

L'emergere di nuove tecnologie digitali, quali l'intelligenza artificiale, l'Internet delle cose e la robotica, pone nuove sfide in termini di sicurezza dei prodotti e di responsabilità, dovute a caratteristiche quali la connettività, l'autonomia, la dipendenza dai dati, l'opacità, la complessità dei prodotti e dei sistemi, l'aggiornamento del software e la maggiore complessità della gestione della sicurezza e delle catene del valore.

La vigente normativa in materia di sicurezza dei prodotti presenta una serie di lacune che devono essere colmate, in particolare la direttiva relativa alla sicurezza generale dei prodotti, la direttiva macchine, la direttiva sulle apparecchiature radio e il nuovo quadro legislativo. I lavori futuri sull'adeguamento di diversi atti normativi di questo quadro saranno effettuati in modo coerente e armonizzato.

Le nuove sfide in termini di sicurezza creano anche nuove sfide in termini di responsabilità. Queste ultime devono essere affrontate al fine di garantire lo stesso livello di protezione concesso alle vittime delle tecnologie tradizionali, mantenendo allo stesso tempo un equilibrio con le esigenze dell'innovazione tecnologica. Ciò contribuirà a creare fiducia nelle nuove tecnologie digitali emergenti e a favorire la stabilità per gli investimenti.

Sebbene in linea di principio le norme vigenti dell'Unione e nazionali in materia di responsabilità siano in grado di far fronte alle tecnologie emergenti, le dimensioni e l'effetto combinato delle sfide poste dall'intelligenza artificiale potrebbero rendere più difficile offrire alle vittime un risarcimento in tutti i casi in cui ciò sia giustificato[63]. Pertanto, l'allocazione dei costi in caso di danni può risultare ingiusta o inefficiente in base alle norme vigenti. Per ovviare a questa situazione e affrontare le potenziali incertezze del quadro vigente, potrebbero essere presi in considerazione alcuni adeguamenti della direttiva sulla responsabilità per danno da prodotti difettosi e dei regimi nazionali in materia di responsabilità attraverso opportune iniziative dell'UE, secondo un approccio mirato e basato sul rischio, vale a dire tenendo conto del fatto che le diverse applicazioni dell'intelligenza artificiale presentano rischi diversi.

[63] Cfr. la relazione della formazione sulle nuove tecnologie, pag. 3, e la raccomandazione politica 27.2 del gruppo di esperti ad alto livello sull'intelligenza artificiale.