

Bryssel den 19.2.2020
COM(2020) 64 final

**RAPPORT FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET, RÅDET OCH
EUROPEISKA EKONOMISKA OCH SOCIALA KOMMITTÉN**

**Konsekvenser för säkerhet och ansvar när det gäller artificiell intelligens, sakernas
internet och robotteknik**

RAPPORT OM KONSEKVENSER FÖR SÄKERHET OCH ANSVAR NÄR DET GÄLLER ARTIFICIELL INTELLIGENS, SAKERNAS INTERNET OCH ROBOTTEKNIK

1. Inledning

Artificiell intelligens (nedan kallad AI)¹, sakernas internet² och robotteknik kommer att skapa nya möjligheter och fördelar för vårt samhälle. Kommissionen har erkänt betydelsen av och potentialen för dessa nya områden och behovet av betydande investeringar inom dem.³ Kommissionen har åtagit sig att göra Europa till världsledande inom AI, sakernas internet och robotteknik. För att uppnå detta mål krävs en tydlig och förutsägbar rättslig ram som riktar in sig på de tekniska utmaningarna.

1.1. Den befintliga ramen för säkerhet och ansvar

Det övergripande syftet med den rättsliga ramen för säkerhet och ansvar är att se till att alla produkter och tjänster, inklusive dem som innehåller ny digital teknik, fungerar på ett säkert, pålitligt och konsekvent sätt och att skador som uppstår effektivt avhjälpas. Höga säkerhetsnivåer för produkter och system som integrerar ny digital teknik och robusta mekanismer för att avhjälpa skador (dvs. ansvarsramen) bidrar till ett bättre konsumentskydd. De skapar också förtroende för tekniken vilket är en förutsättning för att den ska spridas bland användare och inom industrin. Detta kommer i sin tur att öka vår industris konkurrenskraft och bidra till unionens mål⁴. En tydligt fastställd ram för säkerhet och ansvar är särskilt viktigt när det växer fram ny teknik som AI, sakernas internet och robotteknik, både för att skydda konsumenterna och för att säkerställa rättslig förutsebarhet för företagen.

Unionen har en stabil och tillförlitlig rättslig ram för säkerhet och produktansvar och en stor mängd säkerhetsstandarder, kompletterade av nationell, icke-harmoniserad lagstiftning om ansvar. Tillsammans säkerställer de våra medborgares välfärd på den inre marknaden och uppmuntrar innovation och spridning av ny teknik. Dock innebär AI, sakernas internet och robotteknik att särdragen hos många produkter och tjänster förändras.

I kommissionens meddelande Artificiell intelligens för Europa⁵, som antogs den 25 april 2018, meddelade kommissionen att den skulle lägga fram en rapport med en bedömning om vilka konsekvenser den framväxande digitala tekniken har på den befintliga ramen för säkerhet och ansvar. Denna rapport syftar till att identifiera de mer allmänna konsekvenserna av och de potentiella luckorna i ansvars- och säkerhetsramarna för AI, sakernas internet och robotteknik. Riktlinjerna i denna rapport som åtföljer vitboken om AI tillhandahålls i diskussionssyfte och är del i ett bredare samråd med berörda parter. Avsnittet om säkerhet

¹ AI-expertgruppens definition av artificiell intelligens går att hitta på <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>

² Definitionen av sakernas internet går att hitta i rekommendationen ITU-T Y.2060 som finns på <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060>

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

⁴ http://ec.europa.eu/growth/industry/policy_en

⁵ <https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=COM:2018:237:FIN>

Det medföljande arbetsdokumentet från kommissionens avdelningar (2018) 137 (<https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137>) lägger fram en första kartläggning av ansvarsrelaterade utmaningar som uppstår av den framväxande digitala tekniken.

bygger på utvärderingen⁶ av maskindirektivet⁷ och arbetet med de relevanta expertgrupperna⁸. Avsnittet om ansvar bygger på utvärderingen⁹ av direktivet om produktansvar¹⁰, bidrag från expertgrupper¹¹ och kontakter med berörda parter. Syftet med denna rapport är inte att ge en uttömmande översikt över gällande säkerhets- och ansvarsregler utan att fokusera på de viktigaste frågor som hittills har identifierats.

1.2. Särdrag hos AI, sakernas internet och robotteknik

AI, sakernas internet och robotteknik delar många särdrag. De kan kombinera **konnektivitet**, **autonomi** och **uppgiftsberoende** för att utföra uppdrag med begränsad mänsklig kontroll eller översyn eller helt utan mänsklig kontroll eller översyn. System utrustade med AI kan också förbättra sina egna resultat genom att lära sig av sina erfarenheter. Deras **komplexitet** återspeglas både i mångfalden av ekonomiska aktörer som är involverade i **leveranskedjan** och den mångfald av komponenter, delar, programvaror, system och tjänster som tillsammans utgör de nya tekniska ekosystemen. Till detta tillkommer deras **öppenhet** för uppdateringar och uppgraderingar efter att de släppts ut på marknaden. Den stora mängd uppgifter som berörs, beroendet av algoritmer och **bristen på insyn** i AI:s beslutsfattande gör det svårare att förutsäga beteendet hos en produkt med AI-stöd och att förstå de potentiella orsakerna till en skada. Slutligen kan konnektivitet och öppenhet också utsätta AI-produkter och sakernas internet-produkter för **cyberhot**.

1.3. Möjligheter som skapats av AI, sakernas internet och robotteknik

Möjligheten att öka användarnas förtroende för och sociala acceptans av framväxande teknik, att förbättra produkter, processer och affärsmodeller samt att hjälpa de europeiska tillverkarna att bli effektivare är bara några av de möjligheter som skapas genom AI, sakernas internet och robotteknik.

Utöver produktivitets- och effektivitetsvinster innebär AI också en möjlighet för människor att utveckla kunskapsresurser som ännu inte har gått att nå vilket öppnar dörren för nya upptäckter och kan bidra till att lösa några av världens största utmaningar: allt från att behandla kroniska sjukdomar, förutsäga sjukdomsutbrott eller minska dödligheten i trafikolyckor till att bekämpa klimatförändringar eller att förutse cybersäkerhetshot.

⁶ SWD(2018) 161 final.

⁷ Direktiv 2006/42/EG.

⁸ Nätverket för konsumentssäkerhet som inrättades genom direktiv 2001/95/EG om allmän produktsäkerhet samt de expertgrupper som inrättades genom maskindirektivet 2006/42/EG respektive direktiv 2014/53/EU om radioutrustning och som består av medlemsstater, industrin och andra berörda parter som t.ex. konsumentorganisationer.

⁹ COM(2018) 246 final.

¹⁰ Direktiv 85/374/EEG.

¹¹ Expertgruppen för ansvarsfrågor och ny teknik inrättades för att förse kommissionen med sakkunskap om tillämpligheten av direktivet om produktansvar och nationella bestämmelser om skadeståndsansvar samt för att hjälpa kommissionen att utveckla vägledande principer för möjliga sätt att anpassa tillämplig lagstiftning med avseende på ny teknik. Den består av två konstellationer, konstellationen för produktansvar och konstellationen för ny teknik. Se <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1&Lang=SV>

Rapporten från konstellationen för ny teknik *Liability for Artificial Intelligence and other emerging technologies* https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

Tekniken kan medföra många fördelar genom att den kan förbättra produktsäkerheten och minska vissa av produkternas risker. Till exempel skulle uppkopplade och automatiserade fordon kunna förbättra trafiksäkerheten, eftersom de flesta trafikolyckor för närvarande orsakas av mänskliga misstag¹². Dessutom är system för sakernas internet utformade för att ta emot och bearbeta stora mängder data från olika källor. Denna ökade informationsnivå kan komma att användas så att produkterna själva kan anpassa sig och därmed bli säkrare. Ny teknik kan bidra till att produktåterkallelser blir mer effektiva eftersom produkter till exempel skulle kunna varna användarna för att undvika säkerhetsproblem¹³. Om ett säkerhetsproblem uppstår när en ansluten produkt används kan tillverkarna kommunicera direkt med användarna, både för att varna användarna om riskerna och för att, om möjligt, direkt lösa problemet genom att till exempel tillhandahålla en säkerhetsuppdatering. Som ett exempel: 2017, när en smartphonetillverkare återkallade en av sina enheter, skickade tillverkaren ut en programvaruuppdatering för att minska batterikapaciteten hos de återkallade telefonerna¹⁴ till noll så att användarna skulle sluta använda de farliga enheterna.

Dessutom kan ny teknik bidra till att förbättra produkternas spårbarhet. Sakernas internets anslutningsfunktioner kan till exempel göra det möjligt för företag och marknadskontrollmyndigheter att spåra farliga produkter och identifiera risker i leveranskedjorna¹⁵.

Men tillsammans med de möjligheter som AI, sakernas internet och robotteknik kan medföra för ekonomin och våra samhällen kommer också en risk för skador på både materiella och immateriella rättsligt skyddade intressen. Risken för att sådana skador ska uppstå kommer att öka i takt med att tillämpningsområdena blir mer och mer omfattande. I detta sammanhang är det nödvändigt att analysera om och i vilken utsträckning den gällande rättsliga ramen för säkerhet och ansvar fortfarande är lämplig för att skydda användare.

2. Säkerhet

I meddelandet från kommissionen *Att skapa förtroende för människocentrerad artificiell intelligens* fastställs det att **”AI-system [bör] integrera mekanismer för trygghet och inbyggd säkerhet så att de är garanterat säkra i varje steg, med fokus på alla berörda parter fysiska och psykiska säkerhet”**¹⁶.

I bedömningen av unionens lagstiftning om produktsäkerhet i detta avsnitt analyseras huruvida unionens gällande rättsliga ram innehåller de relevanta faktorer som krävs för att säkerställa att ny teknik, och särskilt AI-system, integrerar säkerhet och inbyggd säkerhet.

¹² Man beräknar att omkring 90 % av trafikolyckorna orsakas av mänskliga misstag. Se kommissionens rapport *Rädda liv: öka bilsäkerheten i EU* (COM(2016) 787 final).

¹³ Till exempel kan bilförare ges en varning om att de behöver sänka hastigheten om det inträffat en olycka längre fram.

¹⁴ OECD (2018), ”Measuring and maximising the impact of product recalls globally: OECD workshop report”, *OECD Science, Technology and Industry Policy Papers*, No. 56, OECD Publishing, Paris, <https://doi.org/10.1787/ab757416-en> (ej översatt till svenska).

¹⁵ OECD (2018), ”Enhancing product recall effectiveness globally: OECD background report”, *OECD Science, Technology and Industry Policy Papers*, No. 58, OECD Publishing, Paris, <https://doi.org/10.1787/ef71935c-en> (ej översatt till svenska).

¹⁶ Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén – Att skapa förtroende för människocentrerad artificiell intelligens, Bryssel den 8 april 2019, COM(2019) 168 final.

Denna rapport behandlar främst direktivet om allmän produktsäkerhet¹⁷ samt den harmoniserade produktlagstiftning som följer de övergripande reglerna i den ”nya metoden”¹⁸ och/eller den ”nya lagstiftningsramen” (nedan *unionslagstiftningen om produktsäkerhet* eller *unionens produktsäkerhetsram*)¹⁹. De övergripande reglerna säkerställer samstämmighet mellan de sektorsspecifika reglerna om produktsäkerhet.

Syftet med unionslagstiftningen om produktsäkerhet är att säkerställa att produkter som släpps ut på unionsmarknaden uppfyller höga hälso-, säkerhets- och miljökrav och att sådana produkter kan cirkulera fritt i unionen. Den sektorsspecifika lagstiftningen²⁰ kompletteras av direktivet om allmän produktsäkerhet²¹ där det fastställs att alla konsumentprodukter, även om de inte regleras i unionens sektorsspecifika lagstiftning, måste vara säkra. Säkerhetsbestämmelser kompletteras av marknadskontroll och de befogenheter som tillerkänns de nationella myndigheterna enligt förordningen om marknadskontroll²² och direktivet om allmän produktsäkerhet²³. Inom transportsektorn finns det ytterligare regler på unionsnivå och nationell nivå för att sätta ett motorfordon²⁴, ett luftfartyg eller ett fartyg i drift och tydliga regler som styr säkerheten under drift, inklusive operatörers uppgifter och myndigheters övervakningsåtgärder.

Europeisk standardisering är också en nödvändig del av unionslagstiftningen om produktsäkerhet. Med tanke på digitaliseringens och den framväxande digitala teknikens globala karaktär är det internationella samarbetet om standardisering särskilt relevant för den europeiska industrins konkurrenskraft.

En stor del av unionens produktsäkerhetsram utarbetades före framväxten av digital teknik som AI, sakernas internet och robotteknik. Därför innehåller den inte alltid några bestämmelser som uttryckligen hanterar de nya utmaningar och risker som följer av denna framväxande teknik. Den befintliga produktsäkerhetsramen är dock teknikneutral så detta betyder inte att den inte skulle vara tillämplig på produkter som innehåller denna teknik. I senare rättsakter som ingår i denna ram, som till exempel gäller medicintekniska produkter eller bilar, behandlas dessutom uttryckligen vissa aspekter av utvecklingen av digital teknik, t.ex. automatiserade beslut, programvara som en separat produkt och konnektivitet.

¹⁷ Europaparlamentets och rådets direktiv 2001/95/EG av den 3 december 2001 om allmän produktsäkerhet (EGT L 11, 15.1.2002, s. 4).

¹⁸ EGT C 136, 4.6.1985, s. 1.

¹⁹ Förordning (EG) nr 765/2008 och beslut nr 768/2008/EG.

²⁰ Detta system omfattar inte unionens transport- och billagstiftning.

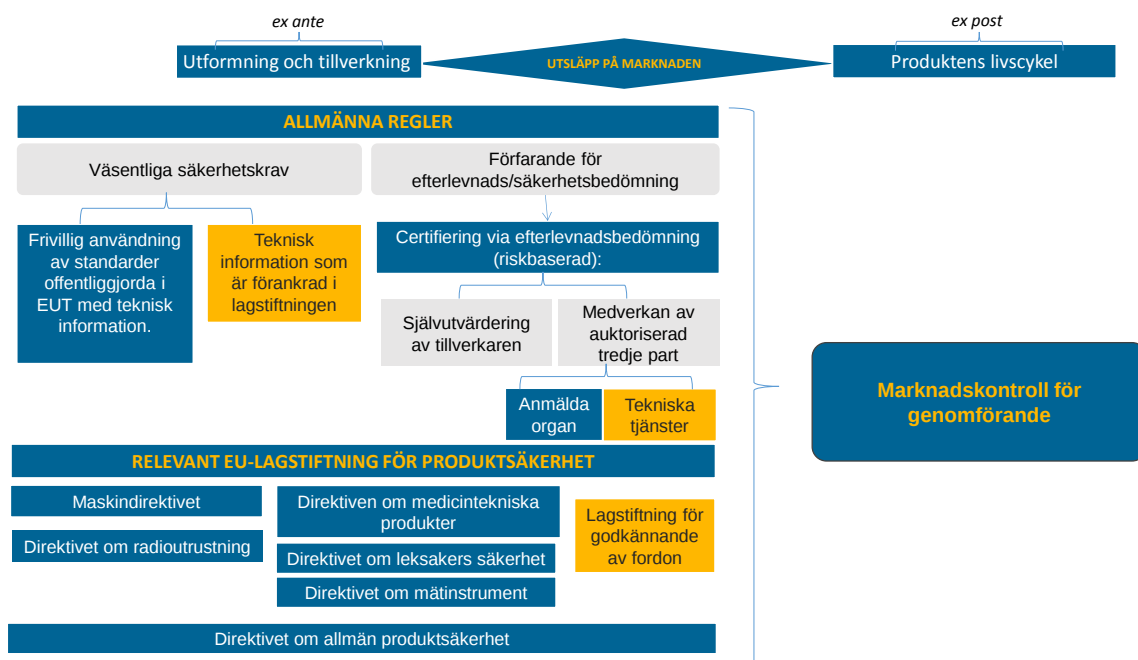
²¹ Europaparlamentets och rådets direktiv 2001/95/EG av den 3 december 2001 om allmän produktsäkerhet (EGT L 11, 15.1.2002, s. 4).

²² Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30) ELI: <http://data.europa.eu/eli/reg/2008/765/oj>, samt från 2021 framåt Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011 (EUT L 169, 25.6.2019, s. 1) ELI: <http://data.europa.eu/eli/reg/2019/1020/oj>

²³ Artikel 8.1 b 3 i direktivet om allmän produktsäkerhet.

²⁴ Till exempel direktiv 2007/46/EG om fastställande av en ram för godkännande av motorfordon och släpvagnar till dessa fordon samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, samt Europaparlamentets och rådets förordning (EU) 2018/858 av den 30 maj 2018 om godkännande av och marknadskontroll över motorfordon och släpfordon till dessa fordon samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, om ändring av förordningarna (EG) nr 715/2007 och (EG) nr 595/2009 samt om upphävande av direktiv 2007/46/EG.

Den underliggande logiken i den gällande unionslagstiftningen om produktsäkerhet²⁵



De utmaningar som den digitala framväxande tekniken innebär för unionens produktsäkerhetsram presenteras nedan.

Konnektivitet är en central funktion i ett växande antal produkter och tjänster. Denna funktion utmanar det traditionella säkerhetsbegreppet eftersom konnektivitet kan äventyra produktens säkerhet direkt, men även indirekt då den kan hackas vilket leder till säkerhetshot och påverkar användarnas säkerhet.

Ett exempel på detta kan hittas i ett meddelande från Island via EU:s system för snabbt informationsutbyte som gällde en smartklocka för barn²⁶. Denna produkt orsakar ingen direkt skada för det barn som bär den, men eftersom den saknar en miniminivå av säkerhet skulle den enkelt kunna användas som ett verktyg för att få tillgång till barnet. Eftersom en av produktens avsedda funktioner är att skydda barn genom att göra dem spårbara skulle en konsument förvänta sig att den inte innebär ett hot mot barns säkerhet genom att de potentiellt kan spåras och/eller kontaktas av vem som helst.

Ett annat exempel går att hitta i ett meddelande som skickats in av Tyskland om en personbil²⁷. Radion i fordonet kan ha vissa säkerhetsluckor i programvaran vilka tillåter obehöriga tredje parter att få åtkomst till de sammanlänkade kontrollsyste- men i fordonet. Om dessa säkerhetsluckor i programvaran utnyttjades av en tredje part i ont uppsåt skulle en trafikolycka kunna inträffa.

Industriella applikationer kan också utsättas för cyberhot som påverkar personsäkerheten i större skala när sådana applikationer saknar den nödvändiga säkerhetsnivån. Detta kan vara fallet till exempel när en cyberattack utförs på ett kritiskt kontrollsyste- m i en industrianläggning i syfte att utlösa en explosion som kan medföra dödsfall.

²⁵ Denna bild omfattar inte kraven i produktlivscykel lagstiftningen, dvs. användning och underhåll, och används bara i illustrationssyfte.

²⁶ Rapexunderrättelse från Island offentliggjord på EU:s webbplats Safety Gate (A12/0157/19).

²⁷ Rapexunderrättelse från Tyskland offentliggjord på EU:s webbplats Safety Gate (A12/1671/15).

Unionslagstiftningen om produktsäkerhet innehåller i allmänhet inte särskilda obligatoriska väsentliga krav för bekämpning av cyberhot som påverkar användarnas säkerhet. Det finns dock bestämmelser om säkerhetsaspekter i förordningen om medicintekniska produkter²⁸, direktivet om mätinstrument²⁹, direktivet om radioutrustning³⁰ och lagstiftningen om typgodkännande av fordon³¹. I cybersäkerhetsakten³² inrättas en frivillig ram för cybersäkerhetscertifiering för produkter, tjänster och processer på informations- och kommunikationsteknikområdet medan det i den relevanta unionslagstiftningen om produktsäkerhet fastställs obligatoriska krav.

Dessutom kan risken för förlust av konnektivitet också innebära risker för den framväxande teknikens säkerhet. Om en uppkopplad brandvarnare förlorar anslutningen kanske den inte varnar användaren om det brinner.

Säkerheten är i den gällande unionslagstiftningen om produktsäkerhet ett offentligpolitiskt mål. Säkerhetsbegreppet är kopplat till produktens användning och till de risker, dvs. mekaniska, elektriska osv, som ska behandlas för att produkten ska bli säker. Det bör noteras att beroende på vilken del av unionens produktsäkerhetslagstiftning det handlar om omfattar produktens användning inte bara den avsedda användningen utan även den förutsebara användningen och i vissa fall, som i maskindirektivet³³, även den rimligen förutsebara felaktiga användningen.

Säkerhetsbegreppet i den gällande unionslagstiftningen om produktsäkerhet är i linje med ett utvidgat säkerhetsbegrepp för att skydda konsumenter och användare. Begreppet produktsäkerhet omfattar alltså skydd mot alla typer av risker som uppstår från en produkt, inte bara mekaniska, kemiska och elektriska, utan också cyberhot och risker kopplade till enheters förlust av anslutning.

Uttryckliga bestämmelser i detta avseende skulle kunna övervägas för de relevanta unionsrättsakternas tillämpningsområde i syfte att ge bättre skydd åt användarna och en ökad rättslig förutsebarhet.

Autonomi³⁴ är ett av de viktigaste inslagen i AI. Oavsedda resultat som har sin grund i AI skulle kunna orsaka skador för användare och utsatta personer.

I den omfattning som AI-produkters framtida ”beteende” kan fastställas på förhand genom den riskbedömning som utförs av tillverkaren innan produkterna släpps ut på marknaden fastställs det redan i unionens produktsäkerhetsram skyldigheter för tillverkaren som innebär

²⁸ Förordning (EU) 2017/745 om medicintekniska produkter.

²⁹ Direktiv 2014/32/EU om tillhandahållande på marknaden av mätinstrument.

³⁰ Direktiv 2014/53/EU om radioutrustning.

³¹ Direktiv 2007/46/EG om typgodkännande av motorfordon och släpvagnar till dessa fordon, samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon. Direktivet kommer från och med den 1 september 2020 att upphävas och ersättas av förordning (EU) 2018/858 om godkännande av och marknadskontroll över motorfordon och släpfordon till dessa fordon samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, om ändring av förordningarna (EG) nr 715/2007 och (EG) nr 595/2009 samt om upphävande av direktiv 2007/46/EG.

³² Förordning (EU) 2019/881.

³³ Direktiv 2006/42/EG om maskiner.

³⁴ Emedan AI-baserade produkter kan agera självständigt genom att uppfatta sin omgivning och utan att följa en uppsättning på förhand fastställda instruktioner, begränsas deras beteende av det mål som de tilldelas och andra relevanta utformningsval som görs av deras utvecklare.

att denna i riskbedömningen ska ta i åtanke ”användningen”³⁵ av produkterna under produkternas livstid. I ramen föreskrivs också att tillverkarna ska tillhandahålla bruksanvisningar och säkerhetsföreskrifter för användare eller varningar³⁶. I denna kontext krävs t.ex. i direktivet om radioutrustning³⁷ att tillverkaren inkluderar bruksanvisningar med information om hur man använder radioutrustningen på avsett vis.

Det kan också finnas situationer i framtiden där resultaten av AI-systemen inte fullt ut kan fastställas på förhand. I en sådan situation kanske den riskbedömning som gjordes innan produkten släpptes ut på marknaden inte längre återspeglar produktens användning, funktion eller beteende. I dessa fall, i den mån som den användning som tillverkaren från början avsett ändras³⁸ på grund av produktens autonoma beteende, och efterlevnaden av säkerhetskraven påverkas, kan det krävas en ny bedömning av den självinlärande produkten³⁹.

Enligt den gällande rättsliga ramen måste tillverkare, när de blir medvetna om att en produkt under sin livscykel medför risker som påverkar säkerheten, omedelbart informera de behöriga myndigheterna och vidta åtgärder för att förebygga riskerna för användarna⁴⁰.

Förutom den riskbedömning som utförs innan en produkt släpps ut på marknaden, skulle ett nytt riskbedömningsförfarande kunna inrättas i de fall där produkten förändras på ett betydande sätt under sin livstid, t.ex. om olika produktfunktioner som inte förutsetts av tillverkaren i den ursprungliga riskbedömningen uppstår. Detta förfarande bör fokusera på den säkerhetspåverkan som orsakats av det autonoma beteendet under produktens livstid. Riskbedömningen bör utföras av lämplig ekonomisk aktör. Dessutom skulle de relevanta unionsrättsakterna kunna omfatta skärpta krav på tillverkare ifråga om bruksanvisningar och varningar för användare.

³⁵ I unionslagstiftningen om produktsäkerhet gör tillverkarna riskbedömningen med utgångspunkt i den avsedda användningen av produkten, den rimligen förutsebara användningen samt den rimligen förutsebara felaktiga användningen.

³⁶ Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG, EUT L 218, 13.8.2008, s. 82. I bilaga I, artikel R2.7 fastställs: ”Tillverkarna ska säkerställa att produkten åtföljs av bruksanvisningar och säkerhetsföreskrifter på ett språk som lätt kan förstås av konsumenter och andra slutanvändare och som bestämts av den berörda medlemsstaten.”

³⁷ Artikel 10.8 som hänvisar till anvisningar till slutanvändaren och bilaga VI som hänvisar till EU-försäkran om överensstämmelse

³⁸ Än så länge används ”självinlärande” i AI-sammanhang mest för att indikera att maskiner kan lära sig under sin träning. Hittills är det inte ett krav att AI-maskiner fortsätter att lära sig efter att de har satts i drift. Särskilt när det gäller hälso- och sjukvård slutar AI-maskiner i regel att lära sig efter det att deras träning framgångsrikt har avslutats. På detta stadium antyder alltså inte det autonoma beteende som härrör från AI-system att produkten utför uppgifter som inte har planerats av tillverkarna.

³⁹ Detta är i linje med avsnitt 2.1 i 2016 års blåbok om genomförandet av EU:s produktbestämmelser.

⁴⁰ Artikel 5 i Europaparlamentets och rådets direktiv 2001/95/EG av den 3 december 2001 om allmän produktsäkerhet.

Liknande riskbedömningar krävs redan i transportlagstiftningen⁴¹. I järnvägstransportlagstiftningen föreskrivs till exempel ett särskilt förfarande när ett järnvägsfordon ändras efter certifieringen. Detta förfarande åläggs ändringens upphovsman och tydliga kriterier definieras för att avgöra om myndigheten behöver vara inblandad eller inte.

AI-produkters och AI-systems självinlärande funktioner kan göra det möjligt för dem att fatta beslut som avviker från vad tillverkarna ursprungligen avsåg och därmed från vad användarna förväntar sig. Detta väcker frågor om behovet av mänsklig kontroll. Människan måste kunna bestämma om AI-produkterna och AI-systemen ska ges behörigheter att fatta beslut och i sådana fall hur, så att de mål som människan har valt kan uppnås⁴². Den befintliga unionslagstiftningen om produktsäkerhet omfattar inte uttryckligen den mänskliga tillsynen inom ramen för AI-produkter och AI-system med självinläring⁴³.

De relevanta unionslagsakterna skulle kunna föreskriva särskilda krav för mänsklig tillsyn, som en skyddsåtgärd, från och med produktutformning och under hela livscykeln för AI-produkter och AI-system.

AI-applikationers framtida ”beteende” skulle kunna innebära **psykiska hälsorisker**⁴⁴ för användare. Dessa psykiska hälsorisker skulle till exempel kunna hänföras till användares kontakter med människoliknande AI-robotar och AI-system hemma och i arbetslivet. I detta avseende används i dag säkerhet i allmänhet för att hänvisa till användarens upplevda hot om fysisk skada som kan komma från den framväxande digitala tekniken. Samtidigt definieras säkra produkter i unionens rättsliga ram som produkter som inte utgör någon risk eller endast en minimal risk för människors säkerhet och hälsa. Det råder enighet om att definitionen av hälsa omfattar både fysisk och psykisk hälsa. Dock bör psykiska hälsorisker uttryckligen omfattas inom begreppet produktsäkerhet i den rättsliga ramen.

Autonomin ska till exempel inte orsaka överdriven stress och överdrivet obehag under långa perioder eller skada psykisk hälsa. I detta sammanhang anses de faktorer som positivt påverkar äldre personers⁴⁵ trygghetskänsla vara att ha trygga relationer med vårdpersonal samt att ha kontroll över dagliga rutiner och informeras om dem. Tillverkare av robotar som

⁴¹ Det förfarande som ska följas vid alla eventuella ändringar av järnvägssystemet som kan påverka säkerheten (t.ex. tekniska och operativa förändringar men också organisatoriska förändringar som skulle kunna påverka processen för drift eller underhåll) går att hitta i bilaga I till kommissionens genomförandeförordning (EU) 2015/1136 (EUT L 185, 14.7.2015, s. 6).

Vid ”väsentliga ändringar” bör en säkerhetsbedömningsrapport lämnas till förslagsställaren av ett oberoende ”bedömningsorgan” (det kan vara den nationella säkerhetsmyndigheten eller en annan tekniskt behörig myndighet).

Efter riskanalysförfarandet kommer förslagsställaren att vidta lämpliga åtgärder för att minska riskerna (om förslagsställaren är ett järnvägsföretag eller en infrastrukturförvaltare är tillämpningen av förordningen en del av dess säkerhetsstyrningssystem, vars tillämpning övervakas av den nationella säkerhetsmyndigheten).

⁴² Policy and Investment Recommendations for Trustworthy AI, AI-expertgruppen, juni 2019 (ej översatt till svenska).

⁴³ Detta utesluter dock inte att tillsyn kan vara nödvändig i en viss situation till följd av några av de befintliga allmänna skyldigheterna avseende utsläppande av en produkt på marknaden.

⁴⁴ Första punktsatsen i WHO:s stadga: ”Hälsa är ett tillstånd av fullständigt fysiskt, psykiskt och socialt välbefinnande och inte blott frånvaro av sjukdom och handikapp” (<https://www.who.int/about/who-we-are/constitution>)

⁴⁵ Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction, s. 237–264, Forskning, Neziha Akalin, Annica Kristoff ersson och Amy Loutfi, juli 2019 (ej översatt till svenska).

interagerar med äldre personer bör ta hänsyn till dessa faktorer för att förebygga risker för psykisk ohälsa.

Det kunde övervägas om den relevanta EU-lagstiftningen borde omfatta uttryckliga krav på att tillverkare av bland annat människoliknande AI-robotar explicit beaktar den immateriella skada som deras produkter kan orsaka användare, i synnerhet sårbara användare som t.ex. äldre personer i vårdmiljöer.

Ett annat centralt särdrag hos AI-baserade produkter och system är **uppgiftsberoende**. Uppgifternas tillförlitlighet och relevans är avgörande för att säkerställa att AI-baserade system och produkter fattar de beslut som tillverkaren har avsett.

I unionslagstiftningen om produktsäkerhet behandlas inte uttryckligen de säkerhetsrisker som härrör från felaktiga uppgifter. Dock bör tillverkaren i enlighet med produktens ”användning” under utformnings- och testfasen beakta uppgifternas korrekthet och deras relevans för säkerhetsfunktionerna.

Exempelvis kan ett AI-baserat system som är utformat för att upptäcka specifika föremål ha problem att känna igen dem i skum belysning, så konstruktörer borde inkludera uppgifter från produkttester i både normalt upplysta och dåligt upplysta miljöer.

Ett annat exempel är kopplat till jordbruksrobotar som exempelvis fruktplockningsrobotar som ska hitta mogna frukter på träd eller på marken. Även om de berörda algoritmerna redan uppvisar en korrekt klassificering i över 90 % av fallen kan brister i de dataset som matar dessa algoritmer leda till att robotarna fattar dåliga beslut och därmed skadar ett djur eller en människa.

Frågan uppstår om unionslagstiftningen om produktsäkerhet ska innehålla särskilda krav som beaktar de säkerhetsrisker som härrör från felaktiga uppgifter under formgivningsfasen samt mekanismer för att säkerställa att kvaliteten på uppgifterna bibehålls under användningen av AI-produkterna och AI-systemen.

Brist på insyn är ett annat centralt särdrag hos vissa AI-baserade produkter och system som kan följa av dessas förmåga att förbättra sina resultat genom att lära sig av sina erfarenheter. Beroende på det metodologiska tillvägagångssättet kan AI-baserade produkter och system kännetecknas av olika grader av brist på insyn. Detta kan leda till att systemet har en beslutsprocess som är svår att spåra (den s.k. black box-effekten). Människor behöver kanske inte förstå alla steg i beslutsprocessen, men allteftersom AI-algoritmerna blir mer och mer avancerade och används inom kritiska områden är det avgörande att människor kan förstå hur de algoritmiska beslut som fattas av systemet har nåtts. Detta skulle vara särskilt viktigt för efterhandsbedömningsmekanismen för genomförande eftersom det kommer att göra det möjligt för tillsynsmyndigheterna att spåra ansvaret för AI-systemens beteendemönster och val. Detta erkänns också i meddelandet från kommissionen om att skapa förtroende för människocentrerad artificiell intelligens⁴⁶.

I unionslagstiftningen om produktsäkerhet behandlas inte uttryckligen de ökande risker som härrör från bristen på insyn i algoritmbaserade system. Det är därför nödvändigt att överväga

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

krav på insyn vad gäller algoritmer, samt vad gäller robusthet, ansvarsskyldighet och, när detta är relevant, mänsklig tillsyn och opartiska resultat⁴⁷. Detta är särskilt viktigt för efterhandsbedömningsmekanismen för genomförande och för att bygga upp förtroendet för användningen av tekniken. Ett sätt att ta itu med denna utmaning skulle vara att införa skyldigheter för utvecklare av algoritmer att lämna ut sina utformningsparametrar och metadata för dataset om olyckor skulle inträffa.

Andra risker som kan påverka säkerheten är de som följer av **produkternas och systemens komplexitet**, eftersom olika komponenter, enheter och produkter kan integreras med varandra och påverka varandras funktioner (t.ex. produkter som ingår i ett ekosystem för ett smart hem).

Denna komplexitet hanteras redan i unionens rättsliga ram för säkerhet som hänvisas till i början av detta avsnitt⁴⁸. Särskilt vid riskbedömning av produkten måste tillverkaren överväga den avsedda användningen, den förutsebara användningen samt, när detta är tillämpligt, den rimligen förutsebara felaktiga användningen.

Om tillverkaren räknar med att enheten kommer att vara sammanlänkad och kommer att interagera med andra enheter ska detta beaktas vid riskbedömningen. Användning eller felaktig användning fastställs på grundval av till exempel erfarenheter från tidigare användning av samma typ av produkt, olycksutredningar eller mänskligt beteende.

Systemens komplexitet behandlas också närmare i sektorsspecifik säkerhetslagstiftning som till exempel förordningen om medicintekniska produkter och, i viss mån, i lagstiftningen om allmän produktsäkerhet⁴⁹. En tillverkare av en ansluten enhet som är avsedd att ingå i ett ekosystem i ett smart hem ska rimligen kunna förutse att deras produkter kommer att påverka säkerheten för andra produkter.

Dessutom tar transportlagstiftningen upp denna komplexitet på systemnivå. För bilar, tåg och flygplan sker typgodkännande och certifiering både för varje komponent och för hela fordonet eller luftfartyget. Trafiksäkerhet, luftvärdighet och järnvägens driftskompatibilitet är del i säkerhetsbedömningen. Inom transportsektorn måste system godkännas av en myndighet, antingen på grundval av en tredje parts bedömning av överensstämmelse enligt tydliga tekniska krav, eller efter en demonstration av riskhanteringen. Lösningen är i allmänhet en kombination av produkt- och systemnivån.

I unionslagstiftningen om produktsäkerhet, inklusive i transportlagstiftningen, tas det redan i viss mån hänsyn till produkters eller systems komplexitet för att hantera de risker som kan påverka användarnas säkerhet.

Komplexa system omfattar ofta **programvara**, som är en nödvändig del i ett AI-baserat system. I allmänhet är tillverkaren av slutprodukten skyldig att som en del av den inledande riskbedömningen förutse riskerna med den programvara som är integrerad i produkten när produkten släpps ut på marknaden.

⁴⁷ På grundval av de centrala krav som föreslagits av AI-expertgruppen i deras etiska riktlinjer för tillförlitlig AI: <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>

⁴⁸ Förordning (EG) nr 765/2008 och beslut nr 768/2008/EG samt harmoniserad sektorsspecifik produktsäkerhetslagstiftning, till exempel maskindirektiv 2006/42/EG.

⁴⁹ I artikel 2 i direktivet om allmän produktsäkerhet anges att en säker produkt ska beakta "[p]roduktens inverkan på andra produkter, om det rimligen kan förutses att den kommer att användas tillsammans med andra produkter".

Vissa delar av unionslagstiftningen om produktsäkerhet hänvisar uttryckligen till den programvara som är integrerad i produkten. I maskindirektivet⁵⁰ krävs till exempel att ett fel i styrsystemets programvara inte ska kunna leda till riskfyllda situationer.

I unionslagstiftningen om produktsäkerhet kan uppdateringar av programvara jämföras med underhåll av säkerhetsskäl, förutsatt att uppdateringarna inte avsevärt ändrar en produkt som redan har släppts ut på marknaden och att de inte medför några nya risker som inte ingick i den ursprungliga riskbedömningen. Om uppdateringen av programvaran väsentligt ändrar den produkt som den hämtas ner till kan dock hela produkten betraktas som en ny produkt och efterlevnaden av den relevanta lagstiftningen om produktsäkerhet måste bedömas på nytt vid den tidpunkt då modifieringen genomförs⁵¹.

Unionens sektorsspecifika harmoniserade lagstiftning om produktsäkerhet innehåller i allmänhet inte några särskilda bestämmelser om fristående programvara som släpps ut på marknaden eller som laddas upp efter att produkten har släppts ut på marknaden. Dock behandlar vissa delar av unionslagstiftningen fristående programvara, t.ex. förordningen om medicintekniska produkter. Dessutom kan fristående programvara som laddas upp i anslutna produkter som kommunicerar via vissa radiomoduler⁵² också regleras genom direktivet om radioutrustning via delegerade akter. Enligt direktivet måste vissa klasser eller kategorier av radioutrustning stödja funktioner som säkerställer att utrustningens uppfyllande av kraven inte äventyras när programvaran laddas upp⁵³.

Även om det i unionens produktsäkerhetslagstiftning tas hänsyn till de säkerhetsrisker som härrör från en programvara integrerad i en produkt vid den tidpunkt då produkten släpps ut på marknaden, och eventuella senare uppdateringar som tillverkaren planerar, kan det behövas särskilda och/eller uttryckliga krav på fristående programvara (t.ex. en app som ska hämtas). Särskild hänsyn bör tas till den fristående programvara som säkerställer säkerhetsfunktioner i AI-produkter och AI-system.

Ytterligare skyldigheter för tillverkare kan behövas för att säkerställa att de tillhandahåller funktioner som förhindrar uppladdning av programvara som påverkar säkerheten under AI-produkternas livstid.

Slutligen påverkas den framväxande digitala tekniken av **komplexa värdekedjor**. Denna komplexitet är dock inte ny och inte heller en fråga som enbart kommer av ny framväxande digital teknik som AI och sakernas internet. Detta gäller till exempel produkter som datorer, tjänsteroboter och transportsystem.

Enligt unionens produktsäkerhetsram gör det inte någon skillnad hur komplex värdekedjan är, ansvaret för produktens säkerhet förblir hos den tillverkare som släpper ut produkten på marknaden. Tillverkarna är ansvariga för säkerheten hos slutprodukten inklusive för de delar som är integrerade i produkten, till exempel programvaran i en dator.

Vissa delar av unionslagstiftningen om produktsäkerhet innehåller redan bestämmelser som uttryckligen hänvisar till situationer där flera ekonomiska aktörer är involverade i en produkt innan denna produkt släpps ut på marknaden. Till exempel krävs i hissdirektivet⁵⁴ att den

⁵⁰ Avsnitt 1.2.1 i bilaga I till maskindirektivet

⁵¹ [2016 års blåbok om genomförandet av EU:s produktbestämmelser](#)

⁵² Radiomoduler är elektroniska apparater som sänder och/eller tar emot radiosignaler (Wifi, Bluetooth) mellan två enheter.

⁵³ Artikel 3.3 i direktivet om radioutrustning.

⁵⁴ I enlighet med artikel 16.2 i direktiv 2014/33/EU.

ekonomiska aktör som konstruerar och tillverkar hissen ska förse installatören⁵⁵ med ”all dokumentation och information som krävs för att denne ska kunna kontrollera att hissen är korrekt och säkert installerad och har genomgått provning”. Maskindirektivet innehåller krav på att tillverkare av utrustning förser operatören med anvisningar om hur utrustningen ska monteras ihop med andra maskiner⁵⁶.

I unionslagstiftningen om produktsäkerhet beaktas värdekedjornas komplexitet och flera ekonomiska aktörer åläggs skyldigheter enligt principen om ”delat ansvar”.

Även om tillverkarens ansvar för den slutliga produktsäkerheten har visat sig vara tillräckligt för de nuvarande komplexa värdekedjorna skulle uttryckliga bestämmelser som specifikt kräver samarbete mellan de ekonomiska aktörerna i leveranskedjan och användarna kunna erbjuda rättslig förutsebarhet i ännu mer komplexa värdekedjor. I synnerhet skulle varje aktör i värdekedjan som inverkar på produktsäkerheten (till exempel tillverkare av programvara) och användare (som till exempel modifierar produkten) ta sitt ansvar och förse nästa aktör i kedjan med den information och de åtgärder som krävs.

3. Ansvar

På unionsnivå är produktsäkerhets- och produktansvarsbestämmelser två kompletterande mekanismer för att uppnå samma politiska mål, målet om en fungerande inre marknad för varor, genom att säkerställa höga säkerhetsnivåer, dvs. minimera skaderisken för användare, och tillhandahålla ersättning för skador till följd av defekta varor.

På nationell nivå kompletterar icke-harmoniserade, civilrättsliga ansvarsramar dessa unionsregler genom att säkerställa ersättning för skador som uppstått av olika orsaker (som från produkter och tjänster) och genom att beakta olika ansvariga personer (såsom ägare, operatörer eller tjänsteleverantörer).

Även om en optimering av unionens säkerhetsregler om AI kan bidra till att olyckor undviks kan de dock ändå inträffa. Detta är när skadeståndsansvaret blir aktuellt. Regler om skadeståndsansvar spelar en dubbel roll i vårt samhälle: å ena sidan säkerställer de att personer som drabbats av en skada orsakad av andra får ersättning och å andra sidan tillhandahåller de ekonomiska incitament för den ansvariga parten att undvika att orsaka sådana skador. Ansvarsregler måste alltid skapa en balans mellan att skydda medborgare från skada och att tillåta företag att vara innovativa.

Ansvarsramarna i unionen har fungerat väl. De har grund i den parallella tillämpningen av direktivet om produktansvar (direktiv 85/374/EEG), som harmoniserat tillverkarens ansvar för defekta produkter, och andra nationella ansvarsordningar som inte är harmoniserade.

I direktivet om produktansvar ges ett skyddslager som inte kan hittas i nationella ansvarsordningar som bygger på enbart vållande. Genom direktivet införs ett system där tillverkaren har strikt ansvar för skador som orsakas av en defekt i dennas produkter. Vid fysisk eller materiell skada har den skadelidande rätt till ersättning om han eller hon kan

⁵⁵ I hissdirektivet 2014/33/EU är installatören likvärdig med tillverkaren och måste ta på sig ansvaret för konstruktionen, tillverkningen och installationen av hissen samt utsläpp av hissen på marknaden.

⁵⁶ I maskindirektivet, bilaga I, artikel 1.7.4.2 står följande ”Varje bruksanvisning skall i tillämpliga fall innehålla minst följande information:” ”i) Monterings-, installations- och anslutningsanvisningar för maskinen, inklusive ritningar, diagram och fästansordningar samt uppgift om det chassi eller den anläggning som maskinen skall monteras på”.

bevisa skadan, defekten i produkten (dvs. att produkten inte tillhandahöll den säkerhet som allmänheten har rätt att förvänta sig) och orsakssambandet mellan den defekta produkten och skadan.

I nationella icke-harmoniserade ordningar fastställs regler baserade på culpaansvar, enligt vilka skadelidande för att kunna få bifall för sin skadeståndstalan måste bevisa den ansvariga personens fel eller försummelse, skadan och orsakssambandet mellan felet eller försummelsen och skadan. De innehåller också strikta ansvarsordningar där den nationella lagstiftaren har tilldelat ansvar för en risk till en viss person, utan att offret behöver bevisa fel/defekt eller orsakssamband mellan fel/defekt och skada.

Nationella ansvarsordningar erbjuder dem som lidit skada av produkter och tjänster flera parallella krav på ersättning grundade på vållande eller strikt ansvar. Dessa krav är ofta riktade mot olika ansvariga personer och har olika villkor.

Till exempel har en skadelidande i en bilolycka vanligtvis ett skadeståndskrav grundat på strikt ansvar gentemot bilens ägare (dvs. den som tar ut ansvarsförsäkringen för motorfordon) och ett skadeståndskrav som bygger på vållande gentemot föraren, båda enligt nationell civilrätt, samt också ett skadeståndskrav enligt direktivet om produktansvar mot tillverkaren om bilen hade en defekt.

Enligt de harmoniserade bestämmelserna om motorfordonsförsäkring ska användningen av fordonet vara försäkrad⁵⁷ och försäkringsgivaren är i praktiken alltid den första platsen för krav på ersättning för personskada eller materiell skada. Enligt dessa regler ersätter den obligatoriska försäkringen skadelidande och skyddar den försäkrade personen som i enlighet med nationella civilrättsliga regler⁵⁸ är skyldig att betala skadestånd till följd av olyckan med motorfordonet. Tillverkare omfattas inte av något krav på obligatorisk försäkring enligt direktivet om produktansvar. Självkörande fordon behandlas inte i unionslagstiftningen på annat sätt än icke-självkörande fordon när det gäller motorfordonsförsäkring. Sådana fordon måste, som alla fordon, omfattas av en ansvarsförsäkring för motorfordon från tredje part, vilket är det enklaste sättet för den skadelidande att få ersättning.

Att teckna en lämplig försäkring kan minska de negativa konsekvenserna av olyckor genom att ge den skadelidande en smidig ersättning. Tydliga ansvarsregler hjälper försäkringsbolag att beräkna sina risker och kräva ersättning från den part som är ytterst ansvarig för skadan. Om en olycka till exempel beror på en defekt kan försäkringsgivaren kräva ersättning från tillverkaren efter att försäkringsgivaren har ersatt den skadelidande.

Särdragen hos framväxande digital teknik som AI, sakernas internet och robotteknik utmanar emellertid delar av unionens och medlemsstaternas ansvarsramar och kan komma att minska deras effektivitet. Vissa av dessa särdrag skulle kunna göra det svårt att spåra skadan tillbaka till ett mänskligt beteende som skulle motivera ett skadeståndskrav som bygger på vållande i enlighet med nationella regler. Detta innebär att skadeståndskrav som grundar sig på nationella skadeståndslagar kan vara svåra eller alltför kostsamma att bevisa och därmed kanske skadelidande inte får tillräcklig ersättning. Det är viktigt att de som lider skador från produkter och tjänster, inklusive från framväxande digital teknik som AI, inte åtnjuter en lägre skyddsnivå jämfört med liknande andra produkter och tjänster för vilka de skulle få ersättning enligt nationella skadeståndslagar. Detta kan minska samhällets acceptans av sådan framväxande teknik och leda till tveksamhet inför användningen.

⁵⁷ Harmoniserade för motorfordon genom direktiv 2009/103/EG om ansvarsförsäkring för motorfordon och kontroll av att försäkringsplikten fullgörs beträffande sådan ansvarighet.

⁵⁸ I de flesta medlemsstater tillämpas strikt ansvar på den person i vars namn motorfordonet är registrerat.

Man måste bedöma om de utmaningar som den nya tekniken innebär för de befintliga ramarna också skulle kunna orsaka rättsosäkerhet om hur de befintliga lagarna ska tillämpas (hur skulle t.ex. begreppet fel eller försummelse tillämpas på skador som orsakats av AI). Dessa skulle i sin tur kunna avskräcka från investeringar och öka informations- och försäkringskostnaderna för tillverkare och andra företag i leveranskedjan, speciellt för europeiska små och medelstora företag. Om medlemsstaterna så småningom skulle hantera de utmaningar som de nationella ansvarsramarna står inför skulle det dessutom kunna leda till ytterligare fragmentering och därmed öka kostnaderna för att driftsätta innovativa AI-lösningar och minska den gränsöverskridande handeln på den inre marknaden. Det är viktigt att företagen känner till sina ansvarsrisker genom hela värdekedjan och kan minska eller förebygga dem och försäkra sig mot dem på ett effektivt sätt.

I detta kapitel förklaras hur ny teknik utmanar de befintliga ramarna och hur dessa utmaningar skulle kunna hanteras. Dessutom kan särdragen inom vissa sektorer, t.ex. hälso- och sjukvård, kräva ytterligare överväganden.

Produkters, tjänsters och värdekedjans komplexitet: Teknik och industri har genomgått en drastisk utveckling under de senaste årtiondena. I synnerhet är kanske skiljelinjen mellan produkter och tjänster inte lika tydlig som den en gång var. Produkter och tillhandahållande av tjänster sammanflätas allt mer. Även om komplexa produkter och värdekedjor inte är nya för den europeiska industrin eller dess regleringsmodell, behöver programvara och även AI särskild uppmärksamhet när det gäller produktansvar. Programvara är en nödvändig del av ett stort antal produkter och kan påverka deras säkerhet. Den är integrerad i produkter men den kan också tillhandahållas separat för att göra det möjligt att använda produkten på avsett vis. Varken en dator eller en smartphone skulle vara särskilt användbar utan programvara. Detta innebär att programvara kan göra en materiell produkt defekt och leda till fysisk skada (jfr med rutan om programvara i avsnittet om säkerhet). Detta skulle i slutändan kunna leda till att tillverkaren av produkten blir ansvarsskyldig i enlighet med direktivet om produktansvar.

Eftersom det finns så många olika typer av programvara är dock inte klassificeringen av programvara som en produkt eller tjänst alltid helt okomplicerad. Medan programvara som styr driften av en konkret produkt kan anses utgöra en del eller en komponent av den produkten, kan det vara svårare att klassificera vissa former av fristående programvara.

Även om produktdefinitionen i direktivet om produktansvar är bred, skulle dess tillämpningsområde kunna förtydligas ytterligare för att bättre återspegla den framväxande teknikens komplexitet och säkerställa att ersättning alltid är tillgänglig för skador som orsakats av produkter som är defekta på grund av programvara eller andra digitala funktioner. Detta skulle göra det lättare för ekonomiska aktörer, t.ex. programvaruutvecklare, att bedöma om de kan betraktas som tillverkare i enlighet med direktivet om produktansvar.

AI är ofta integrerat i komplexa **miljöer för sakernas internet**, där många olika anslutna enheter och tjänster interagerar. Kombinationen av olika digitala komponenter i ett komplext ekosystem och mångfalden av aktörer som är inblandade kan göra det svårt att bedöma var en potentiell skada har uppkommit och vem som är ansvarsskyldig för den. På grund av teknikens komplexitet kan det vara mycket svårt för skadelidande att identifiera den ansvariga personen och bevisa alla nödvändiga förutsättningar för ett framgångsrikt skadeståndskrav i enlighet med nationell lagstiftning. Kostnaderna för denna sakkunskap kan innebära ekonomiska hinder för skadelidande och avskräcka dem från att kräva ersättning.

Dessutom kommer produkter och tjänster som är beroende av AI att interagera med traditionell teknik vilket för mer sig ännu mer komplexitet också när det gäller ansvar. Självkörande bilar kommer till exempel att dela vägar med traditionella bilar under en viss

tid. Liknande komplexitet bland samverkande aktörer kommer att uppstå i vissa tjänstesektorer (t.ex. trafikledning och hälso- och sjukvård) där delvis automatiserade AI-system kommer att stödja mänskligt beslutsfattande.

Enligt rapporten⁵⁹ från konstellationen för ny teknik i expertgruppen för ansvarsfrågor och ny teknik skulle man kunna överväga att anpassa den nationella lagstiftningen för att underlätta bevisbördan för personer som lidit skador kopplade till AI. Bevisbördan kan exempelvis kopplas till (en relevant operatörs) efterlevnad av specifika cybersäkerhetsrelaterade skyldigheter eller andra säkerhetsrelaterade skyldigheter enligt lag: om man inte följer dessa regler skulle en ändring av bevisbördan när det gäller fel eller försummelse och orsakssamband kunna tillämpas.

Kommissionen vill få in synpunkter på om och i vilken utsträckning det finns ett behov av att minska konsekvenserna av komplexiteten genom att minska/omvända den bevisbörda som krävs enligt nationella ansvarsregler avseende skador som orsakats av användningen av AI-applikationer, genom ett lämpligt EU-initiativ.

I unionslagstiftningen skulle en produkt som inte uppfyller de obligatoriska säkerhetsbestämmelserna i enlighet med direktivet om produktansvar anses vara defekt oavsett tillverkarens fel eller försummelse. Det kan emellertid också finnas skäl att överväga sätt att förenkla bevisbördan för skadelidande inom ramen för direktivet. Direktivet bygger på nationella regler om bevisning och orsakssamband.

Konnektivitet och öppenhet: Det är för närvarande inte helt tydligt vilka förväntningar man kan ha på säkerheten när det gäller skador som uppstår till följd av brott mot cybersäkerheten i en produkt och huruvida en sådan skada skulle kompenseras på lämpligt sätt enligt direktivet om produktansvar.

Det kan redan från början finnas brister i cybersäkerheten när en produkt sätts i omlopp, men de kan också uppstå i ett senare skede, långt efter det att produkten sattes i omlopp.

Inom ramarna för culpaansvar innebär fastställande av tydliga skyldigheter för cybersäkerhet att operatörer kan avgöra vad de måste göra för att undvika rättsföljder av ansvarsskyldighet.

Inom ramen för direktivet om produktansvar kan det blir mer relevant att fråga sig om en tillverkare kunde ha förutsett vissa ändringar med hänsyn till produktens rimligen förutsebara användning. Till exempel kanske det blir en ökad användning av det s.k. ”later defect defence” (försvaret om senare defekt), enligt vilket en tillverkare inte är ansvarig om defekten inte fanns när produkten sattes i omlopp, eller ”development risk defence” (försvaret om utvecklingsrisk), dvs. att man baserat på de senaste rönen vid den tidpunkten inte kunde ha förutsett defekten. Dessutom kan ansvarsskyldigheten minska om den skadelidande inte genomför säkerhetsrelaterade uppdateringar. Detta kan eventuellt anses utgöra medvållande från den skadelidandes sida och därmed minska en tillverkares ansvar. Eftersom begreppet förutsebar rimlig användning och frågor om medvållande, som till exempel underlåtenhet att hämta en säkerhetsuppdatering, kan bli vanligare, kan skadelidande uppleva att det är svårare att få ersättning för skador som orsakats av en defekt i en produkt.

Autonomi och brist på insyn: När AI-applikationer kan agera självständigt utför de en uppgift utan att varje steg är förbestämt och med mindre eller så småningom helt utan

⁵⁹ Liability for Artificial Intelligence and other emerging technologies (ej översatt till svenska): https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

omedelbar mänsklig kontroll eller övervakning. Algoritmer som bygger på maskininlärning kan vara näst intill omöjliga att förstå (den s.k. black box-effekten).

Utöver den komplexitet som diskuteras ovan skulle det på grund av bristen på insyn i viss AI kunna bli svårt att få ersättning för skador som orsakas av autonoma AI-applikationer. Behovet av att förstå algoritmen och de uppgifter som används av AI kräver analytisk kapacitet och teknisk expertis som skadelidande kanske inte har råd med. Dessutom kan det vara omöjligt att få tillgång till algoritmen och uppgifterna om den potentiellt ansvariga parten inte samarbetar. I praktiken kan det således hända att skadelidande inte kan kräva skadestånd. Det skulle dessutom vara oklart hur man kan påvisa fel eller försumlighet som orsakats av en AI som agerar autonomt eller vad som skulle anses vara fel eller försummelse av en person som förlitat sig på användning av AI.

Nationella lagar innehåller redan ett antal lösningar för att minska bevisbördan för skadelidande i liknande situationer.

En vägledande princip för unionens produktsäkerhet och produktansvar är att det åläggs tillverkarna att se till att alla produkter som släpps ut på marknaden är säkra under hela sin livscykel och att det ska vara säkert att använda produkterna på det sätt som rimligen kan förväntas. Detta innebär att en tillverkare skulle vara tvungen att se till att en produkt som använder AI följer vissa säkerhetsparametrar. AI:s särdrag utesluter inte att man har rätt att förvänta sig en viss säkerhet av produkter oavsett om de är automatiska gräsklippare eller kirurgiska robotar.

Autonomi kan påverka produktens säkerhet, eftersom autonomin kan innebära att en produkts särdrag väsentligen förändras, inbegripet dess säkerhetsfunktioner. Det handlar om under vilka omständigheter som självinlärande förlänger tillverkarens ansvar och i vilken utsträckning tillverkaren har förutsett vissa förändringar.

I nära samordning med motsvarande ändringar av unionens säkerhetsram skulle begreppet ”sätta i omlopp” som för närvarande används i direktivet om produktansvar kunna ses över med hänsyn till att produkter kan förändras och bli ändrade. Detta kan också bidra till att klargöra vem som är ansvarig för eventuella ändringar som görs av produkten.

Enligt rapporten⁶⁰ från konstellationen för ny teknik i expertgruppen för ansvarsfrågor och ny teknik kan driften av vissa autonoma AI-enheter och AI-tjänster ha en specifik riskprofil när det gäller ansvar, eftersom de kan orsaka betydande skada på viktiga rättsliga intressen som liv, hälsa och egendom, och utsätta allmänheten för risker. Detta kan främst gälla AI-enheter som rör sig på offentliga platser (t.ex. helt självkörande fordon, drönare⁶¹ och paketleveransrobotar) eller AI-baserade tjänster med liknande risker (t.ex. trafikledningstjänster till för att leda eller kontrollera fordon eller styrning av eldistribution). De utmaningar som autonomi och brist på insyn innebär för nationella skadeståndslagar skulle kunna hanteras enligt en riskbaserad strategi. System med strikt ansvar skulle kunna säkerställa att den skadelidande kompenseras när risker materialiseras, oavsett om denna kan påvisa fel eller försummelse. Konsekvenserna av valet om vem som ska ha strikt ansvar inom utveckling och spridning av AI skulle behöva bedömas noggrant och en riskbaserad metod skulle behöva övervägas

⁶⁰ Liability for Artificial Intelligence and other emerging technologies (ej översatt till svenska): https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

⁶¹ Jmf obemannade luftfartygssystem som avses i kommissionens genomförandeförordning (EU) 2019/947 av den 24 maj 2019 om regler och förfaranden för drift av obemannade luftfartyg.

När det gäller användningen av AI-applikationer med en specifik riskprofil vill kommissionen få in synpunkter på om och i vilken utsträckning strikt ansvar, som det används i nationell lagstiftning vad gäller liknande risker som allmänheten utsätts för (till exempel för drift av motorfordon, flygplan eller kärnkraftverk), kan behövas för att eventuella skadelidande faktiskt ska få ersättning. Kommissionen vill också ha synpunkter på en sammanlänkning mellan det strikta ansvaret och en eventuell skyldighet att teckna försäkring, med direktivet om ansvarsförsäkring för motorfordon som förebild, för att säkerställa ersättning oavsett den ansvariga personens solvens och för att bidra till att minska kostnaderna för skador.

För driften av alla andra AI-applikationer, som skulle utgöra det stora flertalet AI-applikationer, överväger kommissionen om bevisbördan när det gäller orsakssamband och fel eller försummelse måste anpassas. En av de frågor som lyfts fram i rapporten⁶² från konstellationen för ny teknik i expertgruppen för ansvarsfrågor och ny teknik gäller de fall där den potentiellt ansvariga parten inte har registrerat de uppgifter som är relevanta för bedömning av ansvar eller inte är villig att dela dess uppgifter med den skadelidande.

4. Slutsats

Framväxten av ny digital teknik som AI, sakernas internet och robotteknik ger upphov till nya utmaningar när det gäller produktsäkerhet och ansvar. Dessa utmaningar handlar om konnektivitet, autonomi, uppgiftsberoende, brist på insyn, produkters och systems komplexitet, programvaruuppdateringar och mer komplex säkerhetshantering och komplexa värdekedjor.

Den gällande lagstiftningen om produktsäkerhet innehåller ett antal luckor som behöver åtgärdas, särskilt i direktivet om allmän produktsäkerhet, maskindirektivet, direktivet om radioutrustning och den nya lagstiftningsramen. Det framtida arbetet med att anpassa olika rättsakter till denna ram kommer att ske på ett konsekvent och harmoniserat vis.

Nya utmaningar i fråga om säkerhet skapar också nya utmaningar i fråga om ansvar. Dessa ansvarsrelaterade utmaningar måste hanteras för att säkerställa samma skyddsnivå som för dem som lidit skada från traditionell teknik, samtidigt som detta balanseras mot behovet av teknisk innovation. Detta kommer att bidra till att skapa förtroende för denna nya framväxande digitala teknik och kommer att skapa investeringsstabilitet.

Emedan den befintliga lagstiftningen om ansvarsskyldighet på unionsnivå och nationell nivå i princip klarar av att hantera den framväxande tekniken kan själva omfattningen och den kombinerade effekten av de utmaningar som härrör från AI göra det svårare att erbjuda ersättning till skadelidande under alla omständigheter där detta skulle vara motiverat⁶³. Därför kan kostnadsfördelningen när skador inträffar inom ramen för de gällande reglerna vara orättvis eller ineffektiv. För att rätta till detta och åtgärda potentiella oklarheter inom den befintliga ramen skulle det gå att överväga att genom lämpliga EU-initiativ göra vissa anpassningar av direktivet om produktansvar och nationella ansvarsordningar med utgångspunkt i en målinriktad, riskbaserad metod, dvs. med beaktande av att olika AI-applikationer medför olika risker.

⁶² Liability for Artificial Intelligence and other emerging technologies (ej översatt till svenska): https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

⁶³ Se rapporten från konstellationen för ny teknik, s. 3, samt policyrekommendationen 27.2 från expertgruppen för ansvarsfrågor och ny teknik.