



Bruxelles, 19.2.2020
COM(2020) 64 final

**RAPORT AL COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU ȘI
COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN**

**Raport privind implicațiile în materie de siguranță și răspundere ale inteligenței
artificiale, ale internetului obiectelor și ale roboticii**

RAPORT PRIVIND IMPLICAȚIILE ÎN MATERIE DE SIGURANȚĂ ȘI RĂSPUNDERE ALE INTELIGENȚEI ARTIFICIALE, ALE INTERNETULUI OBIECTELOR ȘI ALE ROBOTICII

1. Introducere

Inteligența artificială (IA)¹, internetul obiectelor (*Internet of Things* – IoT)² și robotica vor crea noi oportunități și avantaje pentru societatea noastră. Comisia a recunoscut importanța și potențialul acestor tehnologii, precum și necesitatea unor investiții semnificative în aceste domenii³ și este hotărâtă să transforme Europa într-un lider mondial în domeniile IA, IoT și roboticii. Pentru a atinge acest obiectiv, este necesar un cadru juridic clar și previzibil, care să răspundă provocărilor tehnologice.

1.1. Cadrul existent în materie de siguranță și răspundere

Obiectivul general al cadrelor juridice în materie de siguranță și răspundere este de a se asigura că toate produsele și serviciile, inclusiv cele care includ tehnologii digitale emergente, funcționează în condiții de siguranță, în mod fiabil și consecvent și că prejudiciile produse sunt reparate cu eficiență. Existența unor niveluri de siguranță ridicate pentru produsele și sistemele care includ tehnologii digitale noi și crearea unor mecanisme robuste de reparare a prejudiciilor produse (cu alte cuvinte, cadrul în materie de răspundere) contribuie la o mai bună protecție a consumatorilor. Acest lucru creează, de asemenea, încredere în aceste tehnologii, o condiție prealabilă pentru adoptarea lor de către industrie și utilizatori. La rândul său, acest lucru va stimula competitivitatea industriei noastre și va contribui la îndeplinirea obiectivelor Uniunii⁴. Un cadru clar în materie de siguranță și răspundere este deosebit de important atunci când apar noi tehnologii cum ar fi IA, IoT și robotica, pentru a asigura protecția consumatorilor și securitatea juridică pentru întreprinderi.

Uniunea dispune de un cadru de reglementare robust și fiabil în materie de răspundere pentru produse și un set robust de standarde de siguranță, completat de legislații naționale, nearmonizate, privind răspunderea. Împreună, acestea asigură bunăstarea cetățenilor noștri în cadrul pieței unice și încurajează inovarea și adoptarea tehnologiilor noi. Cu toate acestea, IA, IoT și robotica transformă caracteristicile multor produse și servicii.

În Comunicarea privind „Inteligența artificială pentru Europa”⁵, adoptată la 25 aprilie 2018, se anunța intenția Comisiei de a transmite un raport de evaluare a implicațiilor tehnologiilor digitale emergente asupra cadrelor existente în materie de siguranță și răspundere. Scopul acestui raport este de a identifica și a examina implicațiile mai largi și eventualele lacune ale cadrelor în materie de răspundere și siguranță privind IA, IoT și robotica. Orientările cuprinse

¹ Definiția dată inteligenței artificiale de Grupul de experți la nivel înalt privind inteligența artificială (AI HLEG) este disponibilă la adresa <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>.

² Definiția dată internetului obiectelor în Recomandarea ITU-T Y.2060 este disponibilă la adresa <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060>.

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

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

⁵ <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=COM%3A2018%3A237%3AFIN>.

Documentul de lucru însoțitor al serviciilor Comisiei (2018) 137 (<https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137>) a realizat o primă cartografiere a provocărilor în materie de răspundere care intervin în contextul tehnologiilor digitale emergente.

În prezentul raport, care însoțește Cartea albă privind inteligența artificială, sunt oferite spre discuție și fac parte din consultarea mai largă a factorilor interesați. Secțiunea privind siguranța se bazează pe Revizuirea⁶ Directivei privind echipamentele tehnice⁷ și pe colaborarea cu grupurile de experți relevante⁸. Secțiunea privind răspunderea se bazează pe evaluarea⁹ Directivei privind răspunderea pentru produsele cu defect¹⁰, pe contribuțiile grupurilor de experți relevante¹¹ și pe contactele cu părțile interesate. Prezentul raport nu își propune să ofere o imagine de ansamblu exhaustivă a normelor existente în materie de siguranță și răspundere, ci se concentrează asupra aspectelor-cheie identificate până în prezent.

1.2. Caracteristicile tehnologiilor reprezentate de IA, IoT și robotică

IA, IoT și robotica au multe caracteristici comune. Acestea pot combina **conectivitatea**, **autonomia** și **dependența datelor** pentru a efectua sarcini în absența parțială sau totală a controlului și a supravegherii din partea oamenilor. Sistemele echipate cu IA pot, de asemenea, să își amelioreze propriile performanțe învățând din experiență. **Complexitatea** acestor sisteme este dată atât de multitudinea operatorilor economici implicați în **lanțul de aprovizionare**, cât și de multiplicitatea componentelor, a părților, a componentelor de software, a sistemelor și a serviciilor care alcătuiesc împreună noile ecosisteme tehnologice. La aceasta se adaugă **caracterul deschis** la actualizări și modernizări după introducerea lor pe piață. Din cauza cantităților mari de date implicate, a dependenței de algoritmi și a **opacității** procesului decizional al sistemelor cu IA, este mai dificil de anticipat comportamentul unui produs care conține IA și sunt mai greu de înțeles cauzele potențiale ale unui prejudiciu. În fine, conectivitatea și caracterul deschis pot face, de asemenea, ca produsele cu IA sau care țin de IoT să fie mai expuse **amenințărilor cibernetice**.

1.3. Oportunități create de IA, IoT și robotică

Creșterea încrederii utilizatorilor în tehnologiile emergente și a o mai bună acceptare socială a acestora, ameliorarea produselor, a proceselor și a modelelor de afaceri și ajutorul acordat producătorilor europeni pentru a deveni mai eficienți sunt doar câteva dintre oportunitățile create de IA, IoT și robotică.

⁶ SWD(2018) 161 final.

⁷ Directiva 2006/42/CE.

⁸ Rețeaua pentru siguranța consumatorilor, astfel cum a fost instituită prin Directiva 2001/95/CE privind siguranța generală a produselor, Directiva 2006/42/CE privind echipamentele tehnice și Directiva 2014/53/UE privind echipamentele radio, precum și grupuri de experți formați din reprezentanți ai statelor membre, ai industriei și ai altor părți interesate, cum ar fi asociațiile pentru protecția consumatorilor.

⁹ COM(2018) 246 final.

¹⁰ Directiva 85/374/CEE.

¹¹ Grupul de experți privind răspunderea și noile tehnologii a fost creat pentru a se asigura existența în cadrul Comisiei a cunoștințelor de specialitate privind aplicabilitatea Directivei privind răspunderea pentru produsele cu defect și a normelor naționale privind răspunderea civilă, precum și pentru a acorda Comisiei asistență la elaborarea de principii directoare în contextul eventualelor adaptări ale legislației aplicabile având legătură cu noile tehnologii. Grupul este format din două subgrupuri, și anume „subgrupul privind Directiva privind răspunderea pentru produsele cu defect” și „subgrupul privind noile tehnologii”, a se vedea <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewsArch=1&NewSearch=1&Lang=RO>.

Raportul subgrupului privind noile tehnologii având drept obiect răspunderea în domeniul inteligenței artificiale și al altor tehnologii emergente poate fi consultat la adresa https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

Dincolo de creșterea productivității și a eficienței, IA promite, de asemenea, că le va permite oamenilor să dezvolte o inteligență fără precedent, deschizând calea pentru noi descoperiri și contribuind la depășirea unora dintre cele mai mari provocări cu care se confruntă omenirea: de la tratarea bolilor cronice, prevenirea focarelor de boală sau reducerea ratei mortalității în accidente rutiere la combaterea schimbărilor climatice sau anticiparea amenințărilor la adresa securității informatice.

Aceste tehnologii se pot dovedi foarte utile prin ameliorarea siguranței produselor, acestea fiind astfel mai puțin expuse la anumite riscuri. De exemplu, vehiculele automatizate și conectate ar putea îmbunătăți siguranța rutieră, întrucât majoritatea accidentelor sunt în prezent provocate de erori umane¹². În plus, sistemele ținând de IoT sunt concepute pentru a primi și a prelucra cantități mari de date provenite din diverse surse. Acest volum mai mare de informații ar putea fi utilizat pentru ca produsele să se adapteze singure și să devină astfel mai sigure. Noile tehnologii pot contribui la creșterea eficacității rechemărilor produselor, pentru că acestea din urmă ar putea, de exemplu să îi avertizeze pe utilizatori pentru a se evita o problemă de siguranță¹³. Dacă în timpul utilizării unui produs conectat apare o problemă de siguranță, producătorii pot comunica direct cu utilizatorii, pe de o parte pentru a-i avertiza în privința riscurilor, iar pe de altă parte pentru rezolva direct problema, dacă este posibil, de exemplu prin furnizarea unei actualizări vizând asigurarea siguranței. De exemplu, în cursul procesului de rechemare a unuia dintre dispozitivele sale care a avut loc în 2017, un producător de telefoane inteligente a efectuat o actualizare a software-ului pentru a reduce la zero capacitatea bateriei telefoanelor care făceau obiectul rechemării¹⁴, astfel încât utilizatorii să nu mai utilizeze dispozitivele periculoase.

În plus, noile tehnologii pot contribui la ameliorarea trasabilității produselor. De exemplu, datorită conectivității caracteristice IoT, întreprinderile și autoritățile de supraveghere a pieței pot să urmărească produsele periculoase și să identifice riscurile de la nivelul întregului lanț de aprovizionare¹⁵.

Pe lângă oportunitățile pe care IA, IoT și robotica le pot crea pentru economia și societățile noastre, acestea pot să comporte și un risc de prejudiciere a intereselor, atât materiale, cât și imateriale, protejate prin lege. Riscul producerii unor astfel de prejudicii va deveni tot mai mare pe măsură ce domeniul aplicațiilor se va extinde. În acest context, este esențial să se analizeze dacă și în ce măsură actualul cadru juridic privind siguranța și răspunderea este în continuare adecvat pentru protejarea utilizatorilor.

2. Siguranță

În Comunicarea Comisiei intitulată „Consolidarea încrederii în inteligența artificială centrată pe factorul uman” se afirmă că **„sistemele cu IA ar trebui să integreze mecanisme de siguranță și de securitate încă din faza de concepere, astfel încât siguranța lor să poată**

¹² Se estimează că aproximativ 90 % din accidentele rutiere sunt cauzate de erori umane. A se vedea raportul Comisiei intitulat Salvarea de vieți: Sporirea siguranței vehiculelor în UE [COM(2016) 0787 final].

¹³ De exemplu, conducătorul unui autovehicul poate fi avertizat să încetinească dacă pe drumul pe care merge a avut loc un accident.

¹⁴ OCDE (2018), „*Measuring and maximising the impact of product recalls globally: OECD workshop report*”, *OECD Science, Technology and Industry Policy Papers*, Nr. 56, OECD Publishing, Paris, <https://doi.org/10.1787/ab757416-en>.

¹⁵ OCDE (2018), „*Enhancing product recall effectiveness globally: OECD background report*”, *OECD Science, Technology and Industry Policy Papers*, Nr. 58, OECD Publishing, Paris, <https://doi.org/10.1787/ef71935c-en>.

fi verificată în fiecare etapă, punându-se accentul pe siguranța fizică și psihică a tuturor celor implicați¹⁶.

În evaluarea legislației Uniunii privind siguranța produselor realizată în prezenta secțiune se examinează dacă actualul cadru legislativ al Uniunii conține elementele necesare pentru a se asigura că tehnologiile emergente și, în particular, sistemele cu IA, includ caracteristici de siguranță și de securitate de la stadiul concepției.

Prezentul raport examinează în principal Directiva privind siguranța generală a produselor¹⁷ și legislația armonizată privind produsele care respectă normele orizontale ale „noii abordări”¹⁸ și/sau „noul cadru legislativ” (denumite în continuare „Legislația sau cadrul Uniunii privind siguranța produselor”)¹⁹. Normele orizontale asigură coerența normelor sectoriale privind siguranța produselor.

Legislația Uniunii privind siguranța produselor are scopul de a se asigura că produsele introduse pe piața Uniunii respectă cerințe stricte în materie de sănătate, siguranță și protecție a mediului și că aceste produse pot circula liber în întreaga Uniune. Legislația sectorială²⁰ este completată de Directiva privind siguranța generală a produselor²¹, care prevede că toate produsele de consum, chiar și cele care nu sunt reglementate de legislația sectorială a Uniunii, trebuie să fie sigure. Normele de siguranță sunt completate prin supravegherea pieței și prin exercitarea competențelor conferite autorităților naționale de Regulamentul privind supravegherea pieței²² și de Directiva privind siguranța generală a produselor²³. În domeniul transporturilor, există norme suplimentare la nivelul Uniunii și la nivel național pentru punerea în funcțiune a unui autovehicul²⁴, a unei aeronave sau a unei nave, precum și norme clare de reglementare a siguranței în timpul funcționării, inclusiv sarcini care trebuie îndeplinite de operatori și sarcini de supraveghere care le revin autorităților.

Standardizarea europeană este, de asemenea, un element esențial al legislației Uniunii privind siguranța produselor. Având în vedere caracterul mondial al digitalizării și al tehnologiilor

¹⁶ Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor intitulată „Cum construim încrederea cetățenilor într-o inteligență artificială centrată pe factorul uman”, Bruxelles, 8.4.2019, COM(2019) 168 final.

¹⁷ Directiva 2001/95/CE a Parlamentului European și a Consiliului din 3 decembrie 2001 privind siguranța generală a produselor (JO L 11, 15.1.2002, p. 4).

¹⁸ JO C 136, 4.6.1985, p. 1.

¹⁹ Regulamentul (CE) nr. 2008/765 și Decizia (CE) nr. 2008/768.

²⁰ Această schemă nu include legislația Uniunii privind transportul și automobilele.

²¹ Directiva 2001/95/CE a Parlamentului European și a Consiliului din 3 decembrie 2001 privind siguranța generală a produselor (JO L 11, 15.1.2002, p. 4).

²² Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93, JO L 218, 13.8.2008, p. 30, ELI: <http://data.europa.eu/eli/reg/2008/765/oj> și, începând cu anul 2021, Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului din 20 iunie 2019 privind supravegherea pieței și conformitatea produselor și de modificare a Directivei 2004/42/CE și a Regulamentelor (CE) nr. 765/2008 și (UE) nr. 305/2011, JO L 169, 25.6.2019, p. 1, ELI: <http://data.europa.eu/eli/reg/2019/1020/oj>

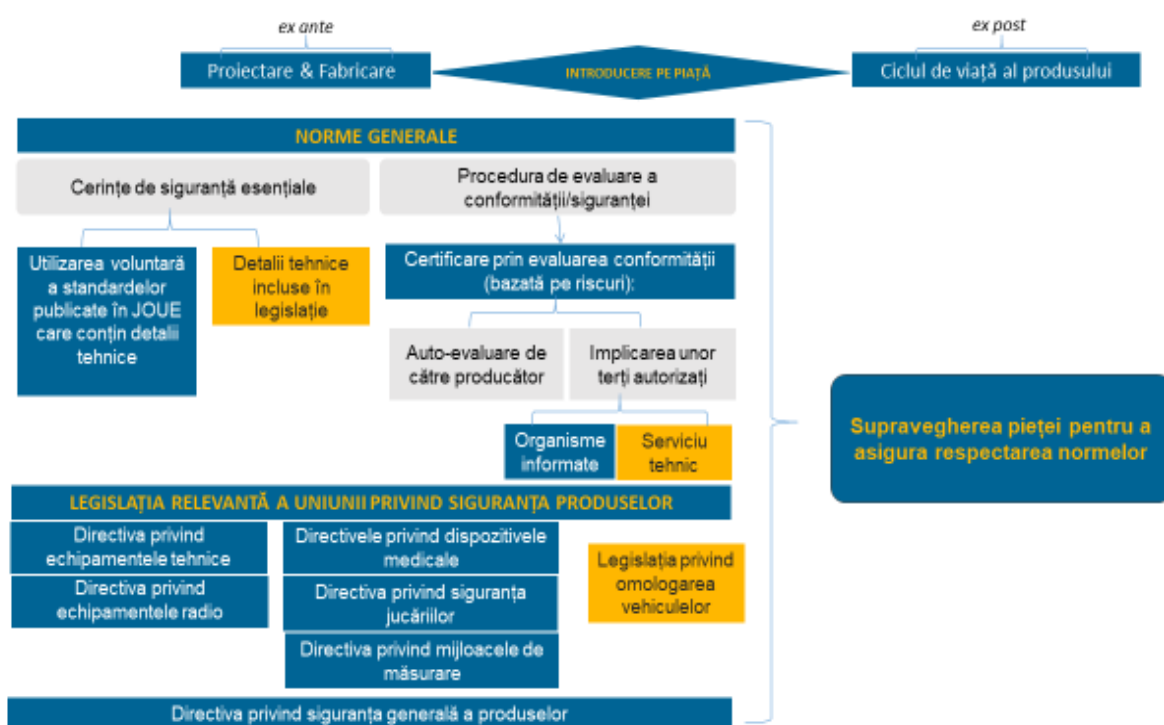
²³ Articolul 8 alineatul (1) litera (b) și articolul 8 alineatul (3) din Directiva privind siguranța generală a produselor.

²⁴ De exemplu Directiva 2007/46/CE privind omologarea autovehiculelor și remorcilor acestora, precum și a sistemelor, componentelor și unităților tehnice separate destinate vehiculelor respective și Regulamentul (UE) 2018/858 al Parlamentului European și al Consiliului din 30 mai 2018 privind omologarea și supravegherea pieței autovehiculelor și remorcilor acestora, precum și ale sistemelor, componentelor și unităților tehnice separate destinate vehiculelor respective, de modificare a Regulamentelor (CE) nr. 715/2007 și (CE) nr. 595/2009 și de abrogare a Directivei 2007/46/CE.

digitale emergente, cooperarea internațională în materie de standardizare este deosebit de relevantă pentru competitivitatea întreprinderilor europene.

Cadrul Uniunii privind siguranța produselor a fost redactat în mare parte înainte de apariția tehnologiilor digitale cum ar fi IA, IoT sau robotica. Prin urmare, acesta nu conține întotdeauna dispoziții care să abordeze în mod explicit provocările și riscurile aferente acestor tehnologii emergente. Cu toate acestea, întrucât cadrul existent în materie de siguranță a produselor este neutru din punct de vedere tehnologic, absența unor dispoziții explicite nu înseamnă că acest cadru nu s-ar aplica și produselor care includ aceste tehnologii. În plus, actele legislative ulterioare care fac parte din acest cadru, cum ar fi cele din domeniul dispozitivelor medicale sau al autoturismelor, au avut deja în vedere în mod explicit anumite aspecte ținând de apariția tehnologiilor digitale, de exemplu deciziile automate, software-ul ca produs separat și conectivitatea.

Logica care să la baza actualei legislații a Uniunii privind siguranța produselor²⁵



Provocările pe care tehnologiile digitale emergente le generează pentru cadrul Uniunii privind siguranța produselor sunt prezentate în continuare.

Conectivitatea este o caracteristică esențială a unui număr tot mai mare de produse și servicii. Această caracteristică reprezintă o provocare pentru conceptul tradițional de siguranță, întrucât conectivitatea poate compromite siguranța unui produs atât în mod direct, cât și în mod indirect – atunci când poate face obiectul unor acte de piraterie care constituie o amenințare la adresa securității și afectează siguranța utilizatorilor.

Un exemplu este notificarea transmisă de Islanda prin sistemul de alertă timpurie al UE, referitoare la un ceas inteligent pentru copii²⁶. Acest produs nu produce un prejudiciu direct copilului care îl poartă, dar, dată fiind absența unui nivel minim de securitate, dispozitivul

²⁵ Această imagine nu include cerințele legislative referitoare la ciclul de viață al produselor, cu alte cuvinte la utilizarea și întreținerea acestora, ci este prezentată doar ca exemplu generic.

²⁶ Notificarea RAPEX din partea Islandei publicată pe site-ul web *Safety Gate* al UE (A12/0157/19).

poate fi utilizat cu ușurință drept instrument pentru a intra în contact cu copilul. Deoarece acest produs își propune, printre altele, să garanteze siguranța copiilor prin localizare, consumatorii se așteaptă ca produsul să nu îi expună pe copii unor riscuri în materie de siguranță prin faptul că aceștia pot fi urmăriți și/sau contactați de oricine.

Un alt exemplu este reprezentat de o notificare transmisă de Germania cu privire la un autoturism²⁷. S-a semnalat că aparatul de radio din autovehicul ar putea avea anumite lacune în materie de securitate la nivelul software-ului, care ar fi putut permite accesul neautorizat al unor terți la sistemele de control interconectate ale autovehiculului. Dacă aceste lacune în materie de securitate de la nivelul software-ului ar fi exploatate de un terț în scopuri rău intenționate, s-ar putea produce un accident.

Aplicațiile industriale care nu au nivelul necesar de securitate pot fi, de asemenea, expuse la amenințări cibernetice, afectând siguranța persoanelor pe o scară mai mare. Un astfel de exemplu ar putea fi atacurile cibernetice asupra sistemului de control cu importanță critică al unei instalații industriale, vizând declanșarea unei explozii care s-ar putea solda cu pierderea unor vieți omenești.

Legislația Uniunii privind siguranța produselor nu prevede, în general, cerințe esențiale obligatorii specifice împotriva amenințărilor cibernetice care afectează siguranța utilizatorilor. Cu toate acestea, există dispoziții având legătură cu securitatea în Regulamentul privind dispozitivele medicale²⁸, în Directiva privind mijloacele de măsurare²⁹, în Directiva privind echipamentele radio³⁰ sau în legislația privind omologarea de tip a vehiculelor³¹. Regulamentul privind securitatea cibernetică³² instituie un cadru voluntar de certificare a securității cibernetice pentru produsele, serviciile și procesele din domeniul tehnologiei informației și comunicațiilor (TIC), în timp ce legislația relevantă a Uniunii privind siguranța produselor prevede cerințe obligatorii în materie.

În plus, riscul pierderii conectivității tehnologiilor digitale emergente poate să implice și riscuri legate de siguranță. De exemplu, dacă o alarmă de incendiu conectată își pierde conectivitatea, este posibil ca utilizatorul să nu mai fie avertizat în caz de incendiu.

Pentru actuala legislație a Uniunii privind siguranța produselor, siguranța reprezintă un obiectiv de politică publică. Conceptul de siguranță are legătură cu utilizarea produsului și cu riscurile, de natură mecanică, electrică etc., care trebuie abordate pentru ca produsul să fie sigur. De remarcat că anumite acte legislative ale Uniunii privind siguranța produselor prevăd că utilizarea produsului include nu numai utilizarea prevăzută, ci și pe cea previzibilă și, în anumite cazuri, cum ar fi cel al Directivei privind echipamentele tehnice³³, chiar și utilizarea anormală previzibilă în mod rezonabil.

²⁷ Notificarea RAPEX din partea Germaniei publicată pe site-ul web *Safety Gate* al UE (A12/1671/15).

²⁸ Regulamentului (UE) 2017/745 privind dispozitivele medicale.

²⁹ Directiva 2014/32/UE, referitoare la punerea la dispoziție pe piață a mijloacelor de măsurare.

³⁰ Directiva 2014/53/UE, privind echipamentele radio.

³¹ Directiva 2007/46/CE, privind omologarea autovehiculelor și remorcilor acestora, precum și a sistemelor, componentelor și unităților tehnice separate destinate vehiculelor respective. Directiva va fi abrogată și înlocuită prin Regulamentul (UE) 2018/858 al Parlamentului European și al Consiliului privind omologarea și supravegherea pieței autovehiculelor și remorcilor acestora, precum și ale sistemelor, componentelor și unităților tehnice separate destinate vehiculelor respective, de modificare a Regulamentelor (CE) nr. 715/2007 și (CE) nr. 595/2009 și de abrogare a Directivei 2007/46/CE, cu efect de la 1 septembrie 2020.

³² Regulamentul (UE) 2019/881.

³³ Directiva 2006/42/CE, privind echipamentele tehnice.

Conceptul de siguranță din actuala legislație a Uniunii privind siguranța produselor este unul extins, vizând protejarea consumatorilor și a utilizatorilor. Astfel, conceptul de siguranță a produselor include protecția împotriva tuturor tipurilor de riscuri generate de produs, înglobând nu numai riscurile mecanice, chimice și electrice, ci și riscurile cibernetice și pe cele legate de pierderea conectivității dispozitivelor.

Ar putea fi avută în vedere includerea unor dispoziții explicite în această privință în actele legislative relevante ale Uniunii, pentru a asigura o mai bună protecție a utilizatorilor și o mai bună securitate juridică.

Autonomia³⁴ este una din principalele caracteristici ale IA. Efectele neintenționate care își au originea în IA le-ar putea provoca prejudicii utilizatorilor și persoanelor expuse.

În măsura în care comportamentul viitor al produselor cu IA poate fi determinat dinainte prin evaluarea riscurilor efectuată de producător înainte de introducerea pe piață a produselor, cadrul Uniunii privind siguranța produselor prevede deja că producătorii sunt obligați să țină cont, atunci când evaluează riscurile, de utilizarea³⁵ produselor de-a lungul întregului ciclu de viață al acestora din urmă. Cadrul prevede, de asemenea, obligația ca producătorii să le furnizeze utilizatorilor instrucțiuni și informații sau avertismente privind siguranța³⁶. În acest context, Directiva privind echipamentele radio³⁷ prevede, de exemplu, obligația producătorului de a include instrucțiuni care să conțină informații privind modul de folosire a echipamentelor radio în conformitate cu utilizarea prevăzută.

Este posibil ca în viitor să existe și situații în care efectele sistemelor cu IA nu vor putea fi pe deplin determinate dinainte. Într-o astfel de situație, este posibil ca evaluarea riscurilor efectuată înainte de introducerea pe piață a produsului să nu mai reflecte utilizarea, funcționarea sau comportamentul acestuia. În aceste cazuri, în măsura în care utilizarea prevăzută inițial de producător suferă modificări³⁸ din cauza comportamentului autonom al produsului, iar respectarea de către acesta a cerințelor de siguranță este afectată, s-ar putea avea în vedere solicitarea unei reevaluări a produsului capabil de învățare autonomă³⁹.

Cadrul actual prevede că în situațiile în care un producător constată că un produs prezintă, la un moment dat de-a lungul ciclului său de viață, riscuri care au un impact asupra siguranței,

³⁴ Deși produsele bazate pe IA pot acționa autonom prin perceperea mediului lor înconjurător, fără a urma un set predeterminat de instrucțiuni, comportamentul acestora este limitat de obiectivul care le-a fost fixat și de alte alegeri relevante în materie de proiectare făcute de dezvoltatorii produselor.

³⁵ În legislația Uniunii privind siguranța produselor, producătorii fac evaluarea riscurilor pe baza utilizării prevăzute a produsului, a utilizării previzibile și a utilizării anormale previzibile în mod rezonabil.

³⁶ Decizia nr. 768/2008/CE a Parlamentului European și a Consiliului din 9 iulie 2008 privind un cadru comun pentru comercializarea produselor și de abrogare a Deciziei 93/465/CEE a Consiliului (JO L 218, 13.8.2008, p. 82). Articolul R2 punctul (7) din anexa I prevede că: „Producătorii se asigură că produsul este însoțit de instrucțiuni și informații privind siguranța, într-o limbă ușor de înțeles pentru consumatori și alți utilizatori finali, după cum se stabilește de către statul membru în cauză.”

³⁷ Articolul 10 alineatul (8), referitor la instrucțiunile pentru utilizatorii finali, și anexa VI, referitoare la declarația de conformitate a UE.

³⁸ Până în prezent, conceptul de „învățare autonomă” a fost utilizat în contextul IA în principal pentru a indica faptul că mașinile sunt capabile să învețe pe parcursul „formării” lor. Nu este încă obligatoriu ca mașinile care utilizează IA să continue să învețe după ce sunt date în funcțiune. Dimpotrivă, în special în domeniul asistenței medicale, mașinile care utilizează IA încetează în mod normal să învețe după ce „formarea” lor s-a finalizat cu succes. Astfel, în stadiul actual, comportamentul autonom având drept sursă sistemele cu IA nu implică faptul că produsul ar efectua sarcini care nu au fost prevăzute de dezvoltatori.

³⁹ Acest lucru este în conformitate cu secțiunea 2.1 din „Ghidul albastru” din 2016 referitor la punerea în aplicare a normelor UE privind produsele.

respectivul producător are obligația de a informa imediat autoritățile competente și de a lua măsuri pentru a preveni riscurile pentru utilizatori⁴⁰.

Pe lângă evaluarea riscurilor efectuată înainte de introducerea unui produs pe piață, ar putea fi instituită o nouă procedură de evaluare a riscurilor în cazurile în care produsul face obiectul unor modificări importante de-a lungul ciclului său de viață, de exemplu prin apariția unei funcții diferite a produsului, neprevăzută de producător în evaluarea inițială a riscurilor. Aceasta ar trebui să se concentreze pe impactul asupra siguranței provocat de comportamentul autonom al produsului de-a lungul ciclului de viață al acestuia. Evaluarea riscurilor ar trebui efectuată de operatorul economic adecvat. În plus, actele legislative relevante ale Uniunii le-ar putea impune producătorilor cerințe mai stricte privind instrucțiunile și avertismentele destinate utilizatorilor.

Evaluări ale riscurilor similare sunt deja prevăzute în legislația privind transporturile⁴¹. De exemplu, în legislația privind transporturile feroviare, dacă un vehicul feroviar face obiectul unor schimbări după ce a fost certificat, autorul schimbării are obligația de a urma o procedură specifică, în care sunt definite criteriile clare pentru a stabili dacă este sau nu nevoie ca autoritatea de resort să fie implicată.

Capacitatea de învățare autonomă a produselor și a sistemelor cu IA poate permite mașinii să ia decizii care se abat de la intențiile inițiale ale producătorilor și, implicit, de la așteptările utilizatorilor. Acest lucru face să se pună problema controlului uman, astfel încât oamenii să poată alege dacă și în ce mod să delege luarea deciziilor către produsele și sistemele cu IA, de așa natură încât să fie îndeplinite obiectivele stabilite de ei înșiși⁴². Legislația existentă a Uniunii privind siguranța produselor nu abordează în mod explicit chestiunea supravegherii umane în contextul produselor și sistemelor cu învățare autonomă care includ AI⁴³.

Actele legislative relevante ale Uniunii pot prevedea cerințe specifice privind supravegherea umană, ca măsură de precauție aplicată, încă de la stadiul de proiectare, de-a lungul întregului ciclu de viață al produselor și sistemelor cu IA.

Comportamentul viitor al aplicațiilor cu IA ar putea genera **riscuri pentru sănătatea mintală**⁴⁴ a utilizatorilor, riscuri care ar decurge, de exemplu, din colaborarea utilizatorilor cu

⁴⁰ Articolul 5 din Directiva 2001/95/CE a Parlamentului European și a Consiliului din 3 decembrie 2001 privind siguranța generală a produselor.

⁴¹ În cazul producerii unor schimbări ale sistemului feroviar care pot avea un impact asupra siguranței (de exemplu schimbări de ordin tehnic, operațional sau organizațional care ar putea avea un impact asupra procesului operațional sau de întreținere), procedura care trebuie urmată este descrisă în anexa I la Regulamentul de punere în aplicare (UE) 2015/1136 al Comisiei (JO L 185, 14.7.2015, p. 6).

În cazul producerii unei „schimbări semnificative”, partea care înaintează propunerea ar trebui să primească din partea unui organism de evaluare independent (care ar putea fi autoritatea națională de siguranță sau o altă entitate competentă din punct de vedere tehnic) un raport de evaluare a siguranței.

În urma procesului de analiză a riscurilor, partea care înaintează propunerea aplică măsurile adecvate de atenuare a riscurilor (dacă partea care înaintează propunerea este o întreprindere feroviară sau un administrator de infrastructură, aplicarea reglementărilor face parte din sistemul său de management al siguranței, a cărui aplicare este supravegheată de ANS).

⁴² Recomandări privind politica și investițiile pentru o IA de încredere, Grupul de experți la nivel înalt privind inteligența artificială, iunie 2019.

⁴³ Acest lucru nu exclude totuși posibilitatea ca supravegherea să fie necesară în anumite situații, ca efect al anumitor obligații mai generale deja existente referitoare la introducerea pe piață a produsului.

⁴⁴ Constituția OMS, primul punct: „sănătatea este o stare generală de bine din punct de vedere fizic, mintal și social, și nu simpla absență a unei boli sau a unei infirmități”. (<https://www.who.int/about/who-we-are/constitution>)

roboți și sisteme umanoide bazate pe IA, acasă sau în mediile de lucru. În această privință, termenul de „siguranță” este în general utilizat în situații în care utilizatorul percepe existența unei amenințări sau a unui prejudiciu fizic care ar putea fi generat de o tehnologie digitală emergentă. În același timp, produsele sigure sunt definite în cadrul juridic al Uniunii ca fiind produse care nu prezintă niciun risc sau care prezintă doar riscuri minime pentru siguranța și sănătatea persoanelor. Conform accepțiunii comune, definiția sănătății include atât bunăstarea fizică, cât și pe cea mentală. Cu toate acestea, riscurile pentru sănătate ar trebui incluse în mod explicit în conceptul de siguranță a produselor din cadrul legislativ.

De exemplu, ar trebui ca autonomia produselor să nu provoace un stres și un disconfort excesiv pentru perioade lungi și să nu afecteze sănătatea mentală. În acest sens, se consideră că factorii care au o influență pozitivă asupra sentimentului de siguranță al persoanelor în vârstă⁴⁵ sunt următorii: existența unor relații sigure cu personalul care asigură asistența medicală, faptul de a avea controlul asupra programului zilnic și faptul de a fi informat în privința acestuia. Producătorii de roboți care interacționează cu persoanele în vârstă ar trebui să țină cont de acești factori, pentru a preveni riscurile pentru sănătatea mentală.

Ar putea fi avute în vedere, pentru a fi incluse în legislația relevantă a UE, obligații explicite pentru producătorii de roboți umanoizi bazați pe IA, de exemplu, de a ține cont de prejudiciile imateriale pe care produsele lor le-ar putea provoca utilizatorilor, în special utilizatorilor vulnerabili, cum ar fi persoanele în vârstă care beneficiază de îngrijire.

O altă caracteristică esențială a produselor și sistemelor bazate pe IA este **dependența datelor**. Exactitatea și relevanța datelor sunt esențiale pentru a se asigura că sistemele și produsele bazate pe IA iau decizii conforme cu intenția producătorului lor.

Legislația Uniunii privind siguranța produselor nu abordează în mod explicit riscurile la adresa siguranței care decurg din date eronate. Cu toate acestea, în funcție de utilizarea produsului, producătorii ar trebui să anticipeze, în cursul fazelor de proiectare și testare, exactitatea datelor și relevanța acestora pentru funcțiile de siguranță.

De exemplu, un sistem bazat pe IA proiectat să detecteze anumite obiecte ar putea avea dificultăți la recunoașterea acestora în condiții slabe de iluminare, prin urmare proiectanții ar trebui să includă date provenite de la testarea produsului atât în medii cu iluminare tipică, cât și în medii cu iluminare slabă.

Un alt exemplu se referă la roboții agricoli, cum ar fi roboții pentru culesul fructelor concepuți pentru a detecta și a localiza fructele coapte în copaci sau la sol. Deși algoritmi utilizați au deja o rată de succes de peste 90 % în ceea ce privește clasificarea, deficiența la nivelul seturilor de date pe care se bazează acești algoritmi poate face ca respectivii roboți să ia o decizie proastă și, astfel, să rănească un animal sau o persoană.

Se pune întrebarea dacă legislația Uniunii privind siguranța produselor ar trebui să conțină cerințe specifice care să abordeze riscurile la adresa siguranței generate de datele eronate încă din faza de proiectare, precum și mecanisme care să asigure menținerea calității datelor pe tot parcursul utilizării produselor și a sistemelor cu IA.

Opacitatea este o altă caracteristică principală a anumitor produse și sisteme bazate pe IA, care ar putea rezulta din capacitatea acestora de a-și ameliora performanțele învățând din experiență. În funcție de abordarea metodologică, produsele și sistemele bazate pe IA pot fi

⁴⁵ *Social Robots: Technological, Societal and Ethical Aspects of Human-Robot Interaction*, pp.237-264, Cercetare, Nezih Akalin, Annica Kristoff ersson și Amy Loutfi, iulie 2019.

caracterizate de diverse grade de opacitate. Acest lucru ar putea face ca procesul decizional al sistemului să fie dificil de trasat (efectul de „cutie neagră”). Oamenii nu au neapărat nevoie să înțeleagă fiecare pas al procesului decizional, dar pe măsură ce algoritmi de IA devin mai avansați și sunt implementați în domenii critice, este esențial ca oamenii să poată înțelege cum au fost luate deciziile algoritmice ale sistemului. Acest lucru ar fi deosebit de important pentru mecanismul *ex post* de asigurare a respectării dispozițiilor, întrucât le-ar da autorităților de resort posibilitatea de a trasa responsabilitățile aferente comportamentelor sistemelor cu IA și alegerilor făcute de acestea. Acest aspect este, de asemenea, recunoscut în Comunicarea Comisiei „Cum construim încrederea cetățenilor într-o inteligență artificială centrată pe factorul uman”⁴⁶.

Legislația Uniunii privind siguranța produselor nu abordează în mod explicit riscurile tot mai mari care decurg din opacitatea sistemelor bazate pe algoritmi. Prin urmare, este necesar să se aibă în vedere cerințe referitoare la transparența algoritmilor, precum și la caracterul robust al acestora, la răspundere și, dacă este cazul, la supravegherea umană și la rezultate nepărtinitoare⁴⁷, fapt deosebit de important pentru mecanismul *ex post* de asigurare a respectării dispozițiilor și pentru consolidarea încrederii în utilizarea acestor tehnologii. O modalitate de abordare a acestor provocări ar fi de a le impune dezvoltatorilor algoritmilor obligația de a face publice parametrii de proiectare și metadatele seturilor de date în cazul producerii unor accidente.

Alte riscuri care ar putea avea un impact asupra siguranței sunt cele care derivă din **complexitatea produselor și a sistemelor**, întrucât diverse componente, dispozitive și produse pot fi integrate și își pot influența reciproc funcționarea (de exemplu produsele care face parte dintr-un ecosistem pentru case inteligente).

Această complexitate este deja abordată în cadrul juridic al Uniunii în materie de siguranță menționat la începutul prezentei secțiuni⁴⁸. În particular, atunci când un producător efectuează evaluarea riscurilor unui produs, trebuie să aibă în vedere utilizarea prevăzută, utilizarea previzibilă și, dacă este cazul, utilizarea anormală previzibilă în mod rezonabil.

În acest context, **dacă producătorul preconizează că dispozitivul său va fi interconectat și va interacționa cu alte dispozitive, acest lucru ar trebui avut în vedere în cadrul evaluării riscurilor**. Utilizarea și utilizarea anormală sunt stabilite, de exemplu, pe baza experienței privind utilizarea anterioară a aceluiași tip de produs, a investigațiilor privind accidentele sau a comportamentului uman.

Complexitatea sistemelor este, de asemenea, abordată în mod mai specific în legislația sectorială în materie de siguranță, cum ar fi Regulamentul privind dispozitivele medicale și, într-o oarecare măsură, în legislația privind siguranța generală a produselor⁴⁹. De exemplu, producătorul unui dispozitiv conectat destinat să facă parte dintr-un ecosistem pentru case inteligente ar trebui să poată anticipa în mod rezonabil că produsele sale vor avea un impact asupra siguranței altor produse.

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

⁴⁷ Pe baza cerințelor-cheie propuse de Grupul de experți la nivel înalt responsabil cu orientările în materie de etică pentru o inteligență artificială (IA) fiabilă: <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines>

⁴⁸ Regulamentul (CE) nr. 2008/765, Decizia (CE) nr. 2008/768 și legislația armonizată sectorială privind siguranța produselor, de exemplu Directiva 2006/42/CE privind echipamentele tehnice.

⁴⁹ Articolul 2 din Directiva privind siguranța generală a produselor prevede că un produs sigur trebuie să ia în considerare „efectul asupra altor produse, în cazurile în care se poate prevedea în mod rezonabil că va fi utilizat împreună cu alte produse”.

În plus, legislația din domeniul transporturilor abordează această complexitate la nivel sistemic. În cazul autoturismelor, al trenurilor și al avioanelor, omologarea de tip și certificarea se realizează în egală măsură pentru întregul vehicul sau întreaga aeronavă și pentru fiecare componentă a acestora. Inspecția tehnică a autovehiculelor și evaluarea navigabilității și a interoperabilității feroviare fac parte din evaluarea siguranței. În domeniul transporturilor, sistemele trebuie să primească o autorizație din partea unei autorități, fie pe baza evaluării de către o terță parte a conformității cu anumite cerințe tehnice clare, fie după demonstrarea modului în care sunt abordate riscurile. Soluția se situează în general parțial la nivelul produsului și parțial la nivelul sistemului.

Legislația Uniunii privind siguranța produselor, inclusiv legislația din domeniul transporturilor, ia deja în considerare, într-o oarecare măsură, complexitatea produselor sau a sistemelor pentru a aborda riscurile care ar putea avea un impact asupra siguranței utilizatorilor.

Sistemele complexe implică adesea o componentă de **software**, care este o parte esențială a unui sistem bazat pe IA. În general, producătorul produsului final are obligația, ca parte a evaluării inițiale a riscurilor, de a prevedea riscurile aferente software-ului integrat în produsul respectiv la momentul introducerii acestuia pe piață.

Anumite acte legislative ale Uniunii privind siguranța produselor se referă în mod explicit la componenta de software integrată în produs. De exemplu, Directiva privind echipamentele tehnice⁵⁰ prevede obligația ca erorile componente de software a sistemului de control să nu conducă la situații periculoase.

În legislația Uniunii privind siguranța produselor, actualizările software-ului ar putea fi comparate cu operațiile de întreținere din motive de siguranță, cu condiția ca actualizările să nu modifice în mod semnificativ un produs deja introdus pe piață și să nu introducă noi riscuri care nu fuseseră prevăzute în evaluarea inițială a riscurilor. Cu toate acestea, dacă actualizarea software-ului modifică în mod substanțial produsul în care este instalat acesta, întregul produs ar putea fi considerat un produs nou, iar conformitatea cu legislația relevantă privind siguranța produselor trebuie reevaluată la momentul efectuării modificării⁵¹.

În cazul unui software autonom introdus pe piață ca atare sau instalat după ce produsul a fost introdus pe piață, legislația sectorială armonizată a Uniunii privind siguranța produselor nu include, în general, dispoziții specifice. Cu toate acestea, anumite acte legislative ale Uniunii includ dispoziții referitoare la software-ul autonom, de exemplu Regulamentul privind dispozitivele medicale. În plus, software-ul autonom instalat în produse conectate care comunică prin intermediul anumitor module radio⁵² poate fi, de asemenea, reglementat de Directiva privind echipamentele radio, prin intermediul unor acte delegate. Directiva prevede că anumite clase sau categorii de echipamente radio să aibă funcții prin care să se asigure că la instalarea de software nu este compromisă conformitatea respectivelor echipamente⁵³.

⁵⁰ Secțiunea 1.2.1 din anexa I la Directiva privind echipamentele tehnice.

⁵¹ [„Ghidul albastru” din 2016 referitor la punerea în aplicare a normelor UE privind produsele](#)

⁵² Modulele radio sunt dispozitive electronice care transmit și/sau recepționează semnale radio (WiFi, Bluetooth) între două dispozitive.

⁵³ Articolul 3 alineatul (3) litera (i) din Directiva privind echipamentele radio.

Legislația Uniunii privind siguranța produselor ia în considerare riscurile de siguranță care derivă din programele informatice integrate într-un produs la momentul introducerii pe piață și, potențial, din actualizările ulterioare prevăzute de producător, dar ar putea fi necesare cerințe specifice și/sau explicite privind software-ul autonom (de exemplu privind aplicațiile care pot fi descărcate). O atenție deosebită ar trebui acordată software-ului autonom care îndeplinește funcții de siguranță în produsele și sistemele cu IA.

Este posibil să fie necesară introducerea unor obligații suplimentare în sarcina producătorilor, pentru a se asigura că aceștia includ caracteristici care să împiedice instalarea unui software cu impact asupra siguranței pe durata de viață a produselor cu IA.

În fine, tehnologiile digitale emergente sunt afectate de **lanțuri valorice complexe**. Această complexitate nu este însă ceva nou și nu este o problemă generată exclusiv de noile tehnologii digitale emergente, cum ar fi IA sau IoT. Același lucru este valabil, de exemplu, în cazul unor produse cum ar fi calculatoarele, roboții care prestează servicii sau sistemele de transport.

În conformitate cu cadrul Uniunii privind siguranța produselor, indiferent de complexitatea lanțului valoric, responsabilitatea pentru siguranța produsului îi revine producătorului care introduce produsul pe piață. Producătorii sunt responsabili de siguranța produsului final, inclusiv în ceea ce privește componentele integrate în produs, de exemplu software-ul unui calculator.

Anumite acte legislative ale Uniunii privind siguranța produselor conțin deja dispoziții care se referă în mod explicit la situații în care mai mulți operatori economici intervin asupra unui anumit produs înainte ca acesta să fie introdus pe piață. De exemplu, Directiva privind ascensoarele⁵⁴ prevede că operatorul economic responsabil de proiectarea și fabricarea unui ascensor trebuie să îi furnizeze instalatorului⁵⁵ „toate documentele și informațiile necesare pentru a-i permite acestuia din urmă să asigure instalarea și testarea corectă și sigură a ascensorului”. Directiva privind echipamentele tehnice prevede obligația producătorilor de echipamente de a-i furniza operatorului informații privind modul de asamblare a echipamentului respectiv cu alte echipamente⁵⁶.

Legislația Uniunii privind siguranța produselor ține cont de complexitatea lanțurilor valorice și impune obligații mai multor operatori economici, în conformitate cu principiul responsabilității partajate.

Responsabilitatea producătorului privind siguranța produsului final s-a dovedit adecvată pentru complexitatea actuală a lanțurilor valorice, dar introducerea unor dispoziții explicite care să impună în mod specific cooperarea dintre operatorii economici din lanțul de aprovizionare și utilizatori ar putea să asigure securitatea juridică inclusiv în lanțuri valorice și mai complexe. În particular, fiecare actor din lanțul valoric care are un impact asupra siguranței produsului (de exemplu producătorii de software), precum și utilizatorii (prin

⁵⁴ În conformitate cu articolul 16 alineatul (2) din Directiva 2014/33/UE.

⁵⁵ Directiva 2014/33/UE, privind ascensoarele, prevede că instalatorul este echivalentul producătorului și că acesta trebuie să își asume responsabilitatea pentru proiectarea, fabricarea, instalarea și introducerea pe piață a ascensorului.

⁵⁶ Anexa I articolul 1.7.4.2 la Directiva privind echipamentele tehnice prevede că „[F]iecare manual de instrucțiuni trebuie să conțină, dacă este cazul, cel puțin următoarele informații: [...] (i) instrucțiunile de asamblare, instalare și conectare, inclusiv desenele, diagramele și modurile de fixare și descrierea șasiului sau instalației pe care echipamentul urmează a fi montat;”.

modificarea produsului) ar urma să își asume responsabilitatea și să furnizeze următorului actor din lanțul de aprovizionare informațiile și măsurile necesare.

3. Răspunderea

La nivelul Uniunii, dispozițiile privind siguranța produselor și răspunderea pentru produse reprezintă două mecanisme complementare care urmăresc același obiectiv, și anume o piață unică a mărfurilor funcțională și caracterizată de un nivel ridicat de siguranță, care să asigure reducerea la minimum a riscului de daune pentru utilizatori și să prevadă despăgubiri pentru prejudiciile provocate de produsele defecte.

La nivel național, cadrele nearmonizate în materie de răspundere civilă completează normele Uniunii, prevăzând compensații pentru prejudicii din diferite surse (produse sau servicii) și permițând obținerea de reparații din partea a diferite categorii de persoane responsabile (proprietari, operatori sau furnizori de servicii).

Deși optimizarea normelor de siguranță ale Uniunii în materie de IA poate contribui la evitarea accidentelor, acestea nu pot fi excluse complet. În astfel de cazuri, intervine răspunderea civilă. Normele privind răspunderea civilă au două funcții în societatea noastră: pe de o parte, garantează că victimele unui prejudiciu cauzat de terți primesc despăgubiri și, pe de altă parte, oferă stimulente economice pentru ca partea responsabilă să evite cauzarea de prejudicii. Normele privind răspunderea trebuie să asigure întotdeauna echilibrul între obiectivul de a-i proteja pe cetățeni și acela de a le permite întreprinderilor să inoveze.

Cadrele în materie de răspundere ale Uniunii au funcționat bine. Acestea se bazează pe aplicarea paralelă a Directivei privind răspunderea pentru produse (Directiva 85/374/CEE), care a armonizat răspunderea producătorului în cazul produselor defecte, și a regimurilor naționale nearmonizate în materie de răspundere.

Directiva privind răspunderea pentru produse oferă un nivel de protecție care nu ar putea fi asigurat doar prin intermediul dispozițiilor la nivel național referitoare la răspunderea bazată pe culpă. Directiva introduce un sistem care prevede răspunderea strictă a producătorului pentru prejudiciile provocate de un defect al produselor sale. În cazul unui prejudiciu fizic sau material, partea vătămată are dreptul la despăgubiri cu condiția să demonstreze prejudiciul, defectul produsului (faptul că acesta nu a oferit siguranța la care se pot aștepta consumatorii) și legătura de cauzalitate dintre produsul defect și prejudiciu.

Regimurile naționale nearmonizate prevăd norme privind răspunderea bazată pe culpă, conform cărora, pentru ca o cerere de despăgubire să fie acceptată, victima prejudiciului trebuie să demonstreze culpa persoanei responsabile, prejudiciul și legătura de cauzalitate dintre defect și prejudiciu. La nivel național există, de asemenea, regimuri de răspundere strictă în cadrul cărora legiuitorul atribuie răspunderea pentru un risc unei persoane specifice, fără a fi necesar ca victima să demonstreze culpa/defectul sau legătura de cauzalitate dintre culpă/defect și prejudiciu.

În temeiul regimurilor naționale în materie de răspundere, victimele unor prejudicii cauzate de produse și servicii pot depune în paralel mai multe cereri de despăgubire, bazate pe fie pe culpă, fie pe răspunderea strictă. Adesea, aceste cereri sunt depuse împotriva unor persoane responsabile diferite și în condiții diferite.

De exemplu, victima unui accident de mașină invocă, de regulă, răspunderea civilă strictă împotriva proprietarului mașinii (mai exact titularul asigurării de răspundere civilă auto) și răspunderea bazată pe culpă împotriva conducătorului auto, ambele în temeiul normelor

naționale de drept civil, însă poate solicita și despăgubiri din partea producătorului, în temeiul Directivei privind răspunderea pentru produse, în cazul în care autoturismul avea un defect.

Potrivit normelor armonizate privind asigurarea autovehiculelor, utilizarea vehiculului trebuie să fie asigurată⁵⁷, iar, în practică, asigurătorul este întotdeauna primul destinatar al cererilor de despăgubire pentru vătămări corporale sau prejudicii materiale. Conform acestor norme, asigurarea obligatorie despăgubește victima și protejează persoana asigurată care, în temeiul normelor naționale de drept civil⁵⁸, trebuie să plătească despăgubiri pentru accidentul în care a fost implicat autovehiculul. Producătorii nu sunt obligați să subscrie la o asigurare în temeiul Directivei privind răspunderea pentru produse. În legislația Uniunii, vehiculele autonome sunt tratate în același mod ca vehiculele neautonome în ceea ce privește asigurarea auto. Vehiculele autonome, la fel ca toate celelalte vehicule, trebuie să fie acoperite de o asigurare de răspundere civilă auto, care reprezintă cea mai simplă modalitate în care partea prejudiciată poate obține despăgubiri.

Încheierea unei asigurări corespunzătoare poate atenua consecințele negative ale accidentelor, asigurând o procedură fiabilă de obținere a despăgubirilor de către victimă. Normele clare privind răspunderea ajută companiile de asigurări să își calculeze riscurile și să solicite rambursarea de la partea care este răspunzătoare în ultimă instanță de prejudiciu. De exemplu, în cazul în care un accident este cauzat de un defect, asigurătorul auto, după ce despăgubește victima, îi poate cere producătorului să îl ramburseze.

Cu toate acestea, caracteristicile tehnologiilor digitale emergente precum IA, IoT și robotica readuc în discuție anumite aspecte ale cadrelor normative naționale și ale Uniunii în materie de răspundere, a căror eficacitate ar putea fi redusă. Unele caracteristici ar putea complica detectarea raportului causal dintre prejudiciu și un comportament uman, pe care ar trebui să se întemeieze cererea de despăgubire bazată pe culpă în conformitate cu normele naționale. Aceasta înseamnă că, în temeiul normelor naționale privind răspunderea civilă, ar putea fi dificil sau excesiv de costisitor să se aducă probe în susținerea cererilor de despăgubire și, prin urmare, ar exista riscul ca victimele să nu primească despăgubiri adecvate. Este important ca victimele accidentelor provocate de produse și servicii care includ tehnologii digitale emergente, precum IA, să beneficieze de un nivel de protecție care să nu fie inferior celui oferit pentru alte produse și servicii similare, pentru care ar obține despăgubiri în temeiul dreptului național al răspunderii civile. În caz contrar, există riscul ca tehnologiile emergente să fie mai puțin acceptate de utilizatori, fapt care ar putea duce la reticență.

Va trebui să se evalueze dacă provocările pe care noile tehnologii le aduc pentru cadrele existente ar putea crea, de asemenea, insecuritate juridică în ceea ce privește modul de aplicare a legislației existente (de exemplu aplicarea conceptului de culpă în cazul prejudiciilor cauzate de IA). Aceste provocări ar putea, la rândul lor, să descurajeze investițiile și să majoreze costurile de informare și de asigurare pentru producători și alte întreprinderi din lanțul de aprovizionare, în special pentru IMM-urile europene. În plus, dacă provocările la adresa cadrelor naționale de răspundere ar fi în cele din urmă soluționate de statele membre, acest lucru ar putea spori fragmentarea, ceea ce ar determina creșterea costurilor de introducere pe piață a soluțiilor de IA inovatoare și reducerea comerțului transfrontalier pe piața unică. Este important ca întreprinderile să cunoască riscurile în

⁵⁷ Armonizate, pentru autovehicule, prin Directiva 2009/103/CE privind asigurarea de răspundere civilă auto și controlul obligației de asigurare a acestei răspunderi.

⁵⁸ În majoritatea statelor membre se aplică răspunderea strictă a persoanei pe numele căreia este înmatriculat autovehiculul.

materie de răspundere la care sunt expuse de-a lungul întregului lanț valoric, să le poată atenua sau preveni și să se asigure în mod eficient împotriva acestora.

Prezentul capitol ilustrează provocările cu care se confruntă cadrele existente din cauza noilor tehnologii și modalitățile în care ar putea fi abordate aceste provocări. În plus, particularitățile anumitor sectoare, cum ar fi asistența medicală, ar putea necesita o evaluare mai aprofundată.

Complexitatea produselor, a serviciilor și a lanțului valoric: tehnologia și industria au evoluat în mod spectaculos în ultimele decenii. În special, linia de demarcație dintre produse și servicii nu mai este la fel de clară ca în trecut. Produsele și furnizarea de servicii sunt tot mai interconectate. Deși produsele și lanțurile valorice complexe nu sunt o noutate pentru industria europeană sau pentru modelul de reglementare a acesteia, software-ul și inteligența artificială merită o atenție specială în ceea ce privește răspunderea pentru produse. Software-ul este esențial pentru funcționarea multor produse, a căror siguranță o pot afecta. Acesta este integrat în produse, dar poate fi, de asemenea, furnizat separat pentru a permite utilizarea produsului în scopul prevăzut. Nici calculatoarele, nici telefoanele inteligente nu pot fi utilizate fără software. Aceasta înseamnă că software-ul poate face ca un produs tangibil să fie defectuos și poate provoca prejudicii fizice (a se vedea rubrica referitoare la software din partea privind siguranța). O astfel de situație ar putea atrage în cele din urmă răspunderea producătorului, în temeiul Directivei privind răspunderea pentru produse.

Cu toate acestea, dat fiind că există multe tipuri și forme de software, încadrarea unui software în categoria serviciilor sau în cea a produselor să nu fie întotdeauna simplă. Astfel, în timp ce software-ul care controlează funcționarea unui produs tangibil ar putea fi considerat o parte sau o componentă a produsului, unele forme de software autonom ar putea fi mai dificil de clasificat.

Deși Directiva privind răspunderea pentru produse oferă o definiție amplă a produselor, domeniul de aplicare al acestei definiții ar trebui clarificat pentru a reflecta mai bine complexitatea tehnologiilor emergente și a garanta că se pot obține despăgubiri în toate cazurile de prejudicii provocate de produse cu defecte legate de software sau de alte caracteristici digitale. Acest lucru le-ar permite operatorilor economici precum dezvoltatorii de software să evalueze mai bine dacă ar putea fi considerați producători în conformitate cu Directiva privind răspunderea pentru produse.

Aplicațiile cu IA sunt adesea integrate în **medii complexe ale IoT**, în care interacționează numeroase dispozitive și servicii conectate. Din cauza combinării diferitor componente digitale într-un ecosistem complex și a pluralității actorilor implicați, poate fi dificil să se evalueze care este sursa unui potențial prejudiciu și persoana responsabilă. Având în vedere complexitatea acestor tehnologii, poate fi foarte dificil pentru victime să identifice persoana responsabilă și să demonstreze că sunt îndeplinite toate condițiile necesare pentru a obține despăgubiri, în conformitate cu legislația națională. Costurile unei astfel de expertize pot fi prohibitive, ceea ce ar putea descuraja victimele să solicite despăgubiri.

În plus, produsele și serviciile care se bazează pe IA vor interacționa cu tehnologiile tradiționale, determinând o complexitate sporită, inclusiv în ceea ce privește răspunderea. De exemplu, pentru un timp, autovehiculele autonome vor circula alături de cele tradiționale. O complexitate similară a interacțiunilor dintre diferiți actori va caracteriza anumite sectoare ale serviciilor (de exemplu gestionarea traficului și sănătatea), în care sisteme cu IA parțial automatizate vor susține procesul de luare a unei decizii de către o persoană.

Conform raportului⁵⁹ elaborat de subgrupul privind noile tehnologii din cadrul Grupului de experți privind răspunderea și noile tehnologii, s-ar putea avea în vedere adaptarea legislațiilor naționale în scopul de a facilita sarcina probei pentru victimele prejudiciilor provocate de IA. De exemplu, sarcina probei ar putea fi legată de respectarea (de către operatorul relevant) a obligațiilor în materie de securitate cibernetică specifice sau a altor obligații în materie de siguranță stabilite prin lege: dacă operatorul nu respectă aceste norme, s-ar putea aplica o modificare a sarcinii probei în ceea ce privește culpa și cauzalitatea.

Comisia solicită opinii pentru a stabili dacă și în ce măsură ar putea fi necesară o atenuare a consecințelor acestei complexități prin diminuarea/inversarea sarcinii probei impuse de normele naționale privind răspunderea pentru prejudiciile provocate de utilizarea aplicațiilor cu IA, printr-o inițiativă adecvată a UE.

În ceea ce privește legislația Uniunii, în conformitate cu Directiva privind răspunderea pentru produse, un produs care nu respectă normele obligatorii de siguranță este considerat defectuos, în mod independent de culpa producătorului. Cu toate acestea, ar putea exista motive pentru a avea în vedere, de asemenea, facilitarea sarcinii probei pentru victime în temeiul directivei, care se bazează pe normele naționale privind probele și stabilirea legăturii de cauzalitate.

Conectivitate și deschidere: deocamdată nu este foarte clar care ar putea fi așteptările în materie de siguranță în cazul prejudiciilor provocate de produse ce nu respectă securitatea cibernetică, nici dacă pentru astfel de daune se pot obține despăgubiri adecvate în temeiul Directivei privind răspunderea pentru produse.

Deficiențele în materie de securitate cibernetică pot exista de la început, când un produs este pus în circulație, dar pot apărea și ulterior, cu mult după punerea sa în circulație.

În cadrul regimurilor de răspundere bazate pe culpă, stabilirea unor obligații clare în materie de securitate cibernetică le permite operatorilor să determine ce trebuie să facă pentru a evita consecințele răspunderii.

În contextul Directivei privind răspunderea pentru produse, ar putea deveni mai important să se stabilească dacă un producător ar fi putut prevedea anumite modificări care să ia în considerare utilizarea previzibilă în mod rezonabil a produsului. De exemplu, s-ar putea recurge mai des la „argumentul defectului ulterior”, potrivit căruia un producător nu este răspunzător dacă defectul nu exista la momentul punerii în circulație, sau la „argumentul riscului de dezvoltare”, potrivit căruia cunoștințele cele mai avansate de la momentul respectiv nu puteau să prevadă defectul. În plus, răspunderea ar putea fi redusă în cazul în care partea vătămată nu efectuează actualizările relevante pentru siguranță. Neefectuarea actualizărilor ar putea fi considerată o neglijență concurentă a persoanei prejudiciate și, prin urmare, ar putea reduce răspunderea producătorului. Având în vedere că noțiunea de utilizare previzibilă în mod rezonabil și chestiunile legate de neglijența concurentă, cum ar fi efectuarea actualizărilor relevante pentru siguranță, ar putea deveni mai importante, persoanelor prejudiciate le-ar putea fi mai greu să obțină despăgubiri în cazul unor prejudicii provocate de un defect al produsului.

Autonomie și opacitate: aplicațiile cu IA care pot funcționa în mod autonom îndeplinesc sarcini fără ca fiecare etapă să fie predefinită, cu mai puțin sau chiar fără control sau

⁵⁹ Raport privind răspunderea legată de inteligența artificială și de alte tehnologii emergente, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

supraveghere umană imediată. Algoritmii bazați pe învățarea automată pot fi dificil de înțeles, dacă nu chiar imposibil (așa-numitul „efect de cutie neagră”).

Pe lângă complexitatea discutată mai sus, efectul de cutie neagră care caracterizează unele tipuri de IA ar putea complica obținerea de despăgubiri pentru prejudiciile provocate de aplicații cu IA autonome. Pentru a înțelege algoritmul și datele utilizate de IA, este nevoie de o capacitate analitică și de o expertiză tehnică ale căror costuri ar putea fi prohibitive pentru victime. În plus, accesul la algoritm și la date ar putea fi imposibil fără cooperarea părții potențial responsabile. Prin urmare, există riscul ca, în practică, victimele să nu poată solicita despăgubiri bazate pe răspundere. De asemenea, nu este clar cum s-ar putea demonstra culpa în cazul unei aplicații cu IA care acționează autonom, nici care ar putea fi considerată a fi culpa unei persoane care se bazează pe utilizarea IA.

Legislațiile naționale au elaborat deja o serie de soluții pentru a reduce sarcina probei pentru victimele aflate în astfel de situații.

În cadrul legislației Uniunii privind siguranța produselor și răspunderea pentru produse, unul dintre principiile de bază este acela că producătorii trebuie să se asigure că toate produsele introduse pe piață sunt sigure pe întreaga durată a ciclului lor de viață, în ceea ce privește utilizările previzibile în mod rezonabil. Aceasta înseamnă că producătorii trebuie să se asigure că produsele care utilizează IA respectă anumiți parametri de siguranță. Caracteristicile IA nu exclud dreptul de a avea așteptări în materie de siguranță a produselor, indiferent dacă acestea sunt mașini automate de tuns iarba sau roboți chirurgicali.

Autonomia poate avea un impact asupra siguranței produsului, deoarece îi poate modifica în mod substanțial caracteristicile, inclusiv cele de siguranță. Întrebarea este în ce condiții caracteristicile de învățare autonomă prelungesc răspunderea producătorului și în ce măsură producătorul ar fi trebuit să prevadă anumite modificări.

Conceptul de „punere în circulație” utilizat în prezent de Directiva privind răspunderea pentru produse ar putea fi revizuit, în strânsă coordonare cu modificările corespunzătoare ale legislației Uniunii în materie de siguranță, pentru a se ține seama de faptul că produsele pot evolua și pot fi modificate. O astfel de revizuire ar putea facilita, de asemenea, stabilirea persoanei responsabile de eventualele modificări aduse produsului.

Conform raportului⁶⁰ elaborat de subgrupul privind noile tehnologii din cadrul Grupului de experți privind răspunderea și noile tehnologii, funcționarea anumitor dispozitive și servicii cu IA autonome ar putea avea un profil de risc specific în ceea ce privește răspunderea, deoarece acestea pot aduce prejudicii semnificative unor interese importante, protejate juridic, precum viața, sănătatea și proprietatea, și pot expune publicul larg la riscuri. Acest lucru ar putea fi valabil în special pentru dispozitivele cu IA care se deplasează în spații publice (vehicule pe deplin autonome, drone⁶¹ sau roboți pentru livrarea coletelor) și pentru serviciile bazate pe IA care prezintă riscuri similare (servicii de gestionare a traficului care conduc sau controlează vehicule, servicii de gestionare a distribuției de energie electrică). Provocările pe care autonomia și opacitatea le aduc în contextul normelor naționale privind răspunderea civilă ar putea fi remediate printr-o abordare bazată pe riscuri. Regimurile de răspundere strictă ar putea garanta că, ori de câte ori se materializează un astfel de risc,

⁶⁰ Raport privind răspunderea legată de inteligența artificială și de alte tehnologii emergente, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

⁶¹ A se vedea sistemele de aeronave fără pilot la bord menționate în Regulamentul de punere în aplicare (UE) 2019/947 al Comisiei din 24 mai 2019 privind normele și procedurile de operare a aeronavelor fără pilot la bord.

victima este despăgubită în mod independent de stabilirea culpei. Ar trebui analizat cu atenție impactul pe care îl vor avea asupra dezvoltării și utilizării IA deciziile cu privire la cine ar trebui să fie strict responsabil pentru astfel de operațiuni.

În ceea ce privește aplicațiile cu IA caracterizate de un profil de risc specific, Comisia solicită opinii pentru a stabili dacă și în ce măsură aplicarea răspunderii stricte, astfel cum este prevăzută de legislația națională în cazul unor riscuri similare la care este expus publicul (de exemplu pentru exploatarea vehiculelor, a avioanelor sau a centralelor nucleare) s-ar putea dovedi necesară pentru a asigura despăgubirea efectivă a victimelor. De asemenea, Comisia solicită opinii cu privire la posibilitatea de a asocia răspunderea strictă cu obligația de a încheia o asigurare disponibilă, după exemplul Directivei privind asigurarea auto, pentru a garanta obținerea de despăgubiri în mod independent de solvabilitatea persoanei responsabile și pentru a contribui la reducerea costurilor prejudiciilor.

Pentru utilizarea tuturor celorlalte aplicații cu IA, care constituie marea majoritate, Comisia analizează dacă sarcina probei ar trebui adaptată în ceea ce privește cauzalitatea și culpa. În acest sens, raportul⁶² elaborat de subgrupul privind noile tehnologii din cadrul Grupului de experți privind răspunderea și noile tehnologii atrage atenția asupra situațiilor în care partea potențial responsabilă nu a înregistrat datele relevante pentru evaluarea răspunderii sau nu este dispusă să i le comunice victimei.

4. Concluzie

Apariția unor noi tehnologii digitale precum IA, internetul obiectelor și robotica ridică noi provocări în ceea ce privește siguranța produselor și răspunderea, cum ar fi conectivitatea, autonomia, dependența datelor, opacitatea, complexitatea produselor și a sistemelor, actualizările de software și complexitatea mai mare a sistemelor de management al siguranței și a lanțurilor valorice.

Legislația actuală privind siguranța produselor prezintă o serie de lacune care trebuie abordate. Este vorba în special de Directiva privind siguranța generală a produselor, de Directiva privind echipamentele tehnice, de Directiva privind echipamentele radio și de noul cadru legislativ. Eforturile viitoare de adaptare a diferitelor acte legislative din acest cadru vor avea loc într-un mod coerent și armonizat.

Noile provocări în materie de siguranță determină, de asemenea, noi provocări în ceea ce privește răspunderea. Acestea vor trebui abordate astfel încât să se asigure același nivel de protecție cu cel de care beneficiază victimele tehnologiilor tradiționale, menținându-se, în același timp, echilibrul în raport cu necesitățile inovării tehnologice. Se va instaura astfel încrederea în tehnologiile digitale emergente și se vor asigura investiții stabile.

Deși, în principiu, normele în materie de răspundere existente la nivelul Uniunii și la nivel național sunt în măsură să răspundă provocărilor legate de noile tehnologii, având în vedere dimensiunea și efectul combinat al acestor provocări ar putea fi dificil să se garanteze că victimele vor obține despăgubiri în toate cazurile în care acest lucru este justificat⁶³. Prin urmare, repartizarea costurilor în caz de prejudiciu în temeiul normelor în vigoare ar putea fi

⁶² Raport privind răspunderea legată de inteligența artificială și de alte tehnologii emergente, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

⁶³ A se vedea raportul elaborat de subgrupul privind noile tehnologii, p. 3, precum și recomandarea de politică 27.2 formulată de Grupul de experți la nivel înalt privind inteligența artificială.

incorectă sau ineficientă. Pentru a remedia această situație și a aborda potențialele incertitudini ale cadrului existent, s-ar putea avea în vedere anumite adaptări, prin inițiative adecvate ale UE, ale Directivei privind răspunderea pentru produse și ale regimurilor naționale în materie de răspundere, pe baza unei abordări specifice bazate pe riscuri, adică o abordare care să țină seama de faptul că diferitele aplicații cu IA prezintă riscuri diferite.