



Bruxelles, 10.1.2017
COM(2017) 9 final

**COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU,
COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN ȘI COMITETUL
REGIUNILOR**

„CONSTRUIREA UNEI ECONOMII EUROPENE A DATELOR”

{SWD(2017) 2 final}

„CONSTRUIREA UNEI ECONOMII EUROPENE A DATELOR”

1. INTRODUCERE

Datele au devenit o resursă esențială pentru creșterea economică, crearea de locuri de muncă și progresul social. Analiza datelor facilitează o mai bună luare a deciziilor, optimizarea proceselor, inovarea și anticiparea evenimentelor viitoare. Această tendință globală are un potențial enorm în diverse domenii, de la sănătate, mediu, securitate alimentară, schimbări climatice și utilizarea eficientă a resurselor până la energie, sisteme de transport inteligente și orașe inteligente.

„Economia datelor”¹ se caracterizează printr-un ecosistem alcătuit din diferite tipuri de actori ai pieței – fabricanți, cercetători și furnizori de infrastructuri – care colaborează pentru ca datele să fie accesibile și utilizabile. Actorii pieței pot astfel să extragă valoare din aceste date, prin crearea unei palete largi de aplicații cu un mare potențial de îmbunătățire a vieții de zi cu zi (de exemplu, gestionarea traficului, optimizarea recoltelor sau furnizarea de servicii de sănătate la distanță).

Valoarea economiei datelor din UE a fost estimată la 257 de miliarde EUR în 2014, adică 1,85 % din PIB-ul UE². Aceasta a crescut la 272 de miliarde EUR în 2015, adică 1,87 % din PIB-ul UE (creștere de 5,6 % față de anul anterior). Conform aceleiași estimări, valoarea ar putea să crească la 643 de miliarde EUR până în 2020, adică 3,17 % din PIB-ul general al UE, dacă se creează la timp condițiile-cadru politice și juridice pentru economia datelor.

După cum se prevede în Regulamentul general privind protecția datelor³, începând din mai 2018 va exista un singur set de norme paneuropene, în loc de 28 de legislații naționale, cum este cazul în prezent. Prin recent creatul mecanism al ghișeului unic⁴ se va asigura că supravegherea operațiunilor de prelucrare transfrontalieră a datelor desfășurate de o societate în UE va intra în domeniul de competență al unei singure autorități pentru protecția datelor. Se va garanta consecvența interpretării noilor norme. În mod concret, în cazurile transfrontaliere în care sunt implicate mai multe autorități naționale pentru protecția datelor va fi adoptată o singură decizie, pentru a se asigura că la problemele

¹ Economia datelor măsoară efectele generale pe care piața datelor – adică piața pe care au loc schimburi de date digitale sub formă de produse sau servicii derivate din date primare – le are asupra economiei în ansamblu. Ea cuprinde generarea, colectarea, stocarea, prelucrarea, distribuirea, analiza, elaborarea, livrarea și exploatarea datelor cu ajutorul tehnologiilor digitale (studiu *European Data Market*, SMART 2013/0063, IDC, 2016).

² Studiu *European Data Market*, SMART 2013/0063, IDC, 2016.

³ Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/56/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

⁴ Articolul 56 din Regulamentul general privind protecția datelor.

comune se găsesc soluții comune. În plus, Regulamentul general privind protecția datelor creează condiții egale pentru întreprinderile din UE și întreprinderile din țări terțe prin faptul că întreprinderile cu sediul în afara UE vor trebui să aplice aceleași reguli ca întreprinderile europene atunci când oferă bunuri și servicii în UE sau când realizează tipare de comportament ale persoanelor din UE. Creșterea nivelului de încredere a consumatorilor va fi atât în avantajul operatorilor comerciali din UE, cât și al celor din afara Uniunii.

Directiva asupra confidențialității și comunicațiilor electronice se referă la confidențialitatea serviciilor de comunicații electronice în UE. Prin versiunea revizuită a Directivei asupra confidențialității și comunicațiilor electronice, propusă în paralel cu prezenta comunicare sub forma unui regulament⁵, se urmărește asigurarea unui nivel ridicat de protecție, în deplină coerență cu Regulamentul general privind protecția datelor. Dacă normele de protecție a datelor sunt solide, se creează încrederea de care economia digitală are nevoie pentru a se dezvolta pe piața internă.

În discursul privind starea Uniunii Europene din 14 septembrie 2016, președintele Juncker a subliniat: *„A fi european înseamnă a avea dreptul ca datele tale cu caracter personal să fie protejate de legi puternice, europene. Pentru că europenilor nu le plac dronele care zboară pe deasupra lor și le înregistrează fiecare mișcare, nici companiile care contabilizează fiecare click pe mouse. De aceea, Parlamentul, Consiliul și Comisia au convenit în mai anul acesta un regulament comun privind protecția datelor cu caracter personal. Acest regulament este o lege europeană fermă aplicabilă companiilor, indiferent de locul în care își au sediul și ori de câte ori prelucrează datele dumneavoastră cu caracter personal. Pentru că, în Europa, păstrarea confidențialității datelor personale contează. Această chestiune ține de demnitatea umană.”*

În Comunicarea „Protecția vieții private într-o lume interconectată – Un cadru european privind protecția datelor pentru secolul 21”⁶ din 2012 și în Comunicarea „Către o economie de succes bazată pe date”⁷ din 2014, Comisia a recunoscut că este nevoie de norme moderne și coerente pe întreg teritoriul UE pentru ca datele să circule liber de la un stat membru la altul și că economia digitală europeană a fost lentă în preluarea revoluției datelor în comparație cu SUA și nici nu a dispus de capacități industriale comparabile. Concluzia a fost că lipsa unui mediu juridic adaptat la comerțul cu date în cadrul UE ar putea explica în parte accesul insuficient la seturi mari de date, posibilele bariere la intrarea pe piață a nou-veniților și descurajarea inovării.

Restricțiile nejustificate asupra liberei circulații a datelor ar putea frâna dezvoltarea economiei datelor în UE. Aceste restricții constau în cerințe impuse de autoritățile publice cu privire la locul de stocare sau de prelucrare a datelor. Problema liberei circulații a datelor se referă la toate tipurile de date: întreprinderile și actorii din economia datelor lucrează cu date industriale și generate de calculatoare, cu caracter personal sau nu, precum și cu date create prin acțiunea umană. În strategia privind piața unică digitală, Comisia a anunțat că va propune o inițiativă de combatere a restricțiilor asupra liberei circulații a datelor care nu au legătură cu protecția datelor cu caracter

⁵ COM(2017) 10.

⁶ COM(2012) 9.

⁷ COM(2014) 442.

personal în UE și de combatere a restricțiilor nejustificate referitoare la locul de stocare sau de prelucrare a datelor. Printre restricțiile de acest fel se numără anumite acte juridice adoptate de statele membre, norme administrative și practici administrative cu același efect. Numărul acestora tinde să se mărească pe măsură ce economia datelor crește, creând astfel incertitudine cu privire la locul unde pot fi stocate sau prelucrate date. Efectele acestor restricții s-ar putea resimți în toate sectoarele economiei și în organizațiile private și publice, cărora le-ar putea fi îngreunat accesul la servicii de date mai inovatoare și/sau mai ieftine. Restricțiile nejustificate referitoare la locul datelor afectează libera prestare a serviciilor și libertatea de stabilire prevăzute în tratat, fiind astfel contrare și legislației secundare relevante. Există astfel riscul unei fragmentări a pieței, al unei reduceri a calității serviciilor oferite utilizatorilor și al unei reduceri a competitivității furnizorilor de servicii de date, în special a entităților mai mici.

Localizarea nejustificată a datelor face parte și din discuțiile purtate de UE cu partenerii săi comerciali, dată fiind importanța crescândă pe care o au datele și serviciile de date în economia globală și având în vedere posibilele atitudini adoptate de țările terțe față de această chestiune. Normele UE în materie de protecție a datelor nu pot face obiectul negocierilor din cadrul unui acord de liber schimb. După cum se explică în Comunicarea „Schimbul de date cu caracter personal și protecția acestora într-o lume globalizată”⁸, dialogurile având ca temă protecția datelor trebuie să urmeze o cale separată de cea a negocierilor comerciale cu țările terțe. În plus, după cum se indică în Comunicarea „Comerț pentru toți”⁹, Comisia va încerca să utilizeze acordurile comerciale ale UE pentru a stabili norme pentru comerțul electronic și fluxurile transfrontaliere de date și pentru a aborda noi forme de protecționism digital, în deplină conformitate cu normele privind protecția datelor în UE și fără a aduce atingere acestor norme.

De altminteri, pe măsură ce transformarea bazată pe date pătrunde în economie și în societate, volume tot mai mari de date sunt generate de calculatoare sau procese bazate pe tehnologii emergente, cum ar fi internetul obiectelor, fabricile viitorului și sistemele autonome conectate. Conectivitatea însăși schimbă modul în care pot fi accesate datele: accesul la date, care avea loc de obicei prin conexiuni fizice, se face în prezent tot mai des de la distanță. Abia încep să se contureze diversitatea enormă a surselor și tipurilor de date și posibilitățile variate de a aplica observațiile făcute pe baza acestor date într-o serie de domenii, cum ar fi elaborarea politicilor publice. Pentru a profita de aceste posibilități, actorii pieței datelor, atât cei publici, cât și cei privați, trebuie să aibă acces la seturi de date mari și diversificate. Accesul la datele generate de calculatoare sau procese și transmisia acestor date sunt, prin urmare, aspecte esențiale pentru crearea unei economii a datelor și necesită o analiză atentă.

Alte întrebări care se profilează sunt în ce măsură se vor aplica normele de răspundere în cazul prejudiciilor rezultate din defecte ale dispozitivelor conectate sau ale roboților și dacă se va asigura portabilitatea și interoperabilitatea datelor. În contextul noilor tehnologii, cum ar fi internetul obiectelor sau robotica, există interdependențe complexe și foarte complicate atât în interiorul produselor (la nivel de hardware și software), cât și între diferitele dispozitive interconectate. Alte probleme ar putea apărea în legătură cu echipamentele autonome, al căror comportament neprevăzut și neintenționat ar putea

⁸ COM(2017) 7.

⁹ COM(2015) 497.

produce prejudicii persoanelor și obiectelor. Aceste fenomene ar putea crea insecuritate juridică în ceea ce privește aplicarea cadrului existent în materie de răspundere și siguranță.

După cum s-a anunțat în strategia privind piața unică digitală, obiectivul Comisiei este acela de a crea un cadru politic și juridic clar și adaptat pentru economia datelor, prin înlăturarea barierelor care blochează încă libera circulație a datelor și prin rezolvarea insecurităților juridice create de noile tehnologii de date. Printre alte obiective care stau la baza prezentei comunicări se numără mărirea volumului de date disponibile și utilizate, promovarea unor modele noi de afaceri în sectorul datelor și îmbunătățirea condițiilor de acces la date și a dezvoltării unor instrumente de cercetare analitică a datelor în UE. În prezenta comunicare, Comisia prezintă o serie de teme centrale de discuție în vederea „construirii unei economii europene a datelor”.

Aceste teme sunt: fluxul liber al datelor, accesul la datele generate de calculatoare și transferul acestora, răspunderea și siguranța în contextul tehnologiilor emergente și portabilitatea datelor fără caracter personal, interoperabilitatea și standardele. Prezenta comunicare conține, de asemenea, câteva sugestii de experimentare a unor soluții de reglementare comune într-un mediu real.

Comisia lansează un amplu dialog cu părțile interesate pentru discutarea aspectelor analizate în prezenta comunicare. Prima etapă a acestui dialog este o consultare publică, lansată în paralel cu pachetul privind economia datelor¹⁰.

2. FLUXUL LIBER AL DATELOR

Pentru a funcționa bine și a fi dinamică, o economie a datelor are nevoie ca fluxul datelor pe piața internă să fie permis și protejat. Într-un context tehnologic cu evoluție rapidă, condiția ca fluxul liber al datelor să fie sigur și fiabil este esențială pentru protecția celor patru libertăți fundamentale ale pieței unice a UE care sunt consacrate în tratate (libera circulație a mărfurilor, a lucrătorilor, a serviciilor și a capitalurilor). Serviciile de date prezintă o creștere rapidă în UE și în lume. Dacă piața unică din acest sector este eficientă și lipsită de bariere, se creează posibilități semnificative de creștere economică suplimentară și noi locuri de muncă.

Creșterea și inovarea în economia datelor și introducerea unor servicii publice transfrontaliere pot fi compromise de barierele din calea liberei circulații a datelor în UE, cum ar fi cerințele nejustificate în materie de localizare a datelor, impuse de autoritățile publice. De fapt, prin măsurile de localizare a datelor se reintroduc „controale la frontieră”, digitale de această dată¹¹. Aceste măsuri pot lua forma unor cerințe, impuse de autoritățile de supraveghere, ca furnizorii de servicii financiare să își stocheze datele la nivel local sau chiar a unor norme privind secretul profesional, care presupun ca datele să fie stocate sau prelucrate la nivel local, și a unor regulamente cu un câmp de aplicare prea vast în care se prevede că sectorul public trebuie să stocheze la nivel local informațiile arhivate pe care le generează, indiferent de sensibilitatea acestora.

¹⁰ <https://ec.europa.eu/digital-single-market/news-redirect/52039>.

¹¹ OCDE, „*Emerging Policy Issues: Localisation Barriers to Trade*”, 2015 și lucrări în curs.

Protecția vieții private este o preocupare legitimă, care nu ar trebui totuși să constituie pentru autoritățile publice un motiv de a restricționa în mod nejustificat fluxul liber al datelor. După cum s-a arătat mai sus, în Regulamentul general privind protecția datelor se prevede un set unic de norme cu un nivel ridicat de protecție a datelor cu caracter personal pentru întreaga UE. Prin acest regulament se mărește încrederea consumatorilor în serviciile online și se asigură aplicarea uniformă a normelor în toate statele membre, ca urmare a consolidării autorităților naționale de protecție a datelor. Regulamentul general privind protecția datelor promovează încrederea necesară pentru prelucrarea datelor și constituie baza pentru fluxul liber al datelor cu caracter personal în UE. Conform Regulamentului general privind protecția datelor, restricțiile asupra liberei circulații a datelor cu caracter personal în interiorul Uniunii sunt interzise atunci când au la bază motive legate de protecția datelor cu caracter personal¹². Restricțiile care au la bază alte motive în afară de protecția datelor cu caracter personal, cum ar fi prevederi fiscale sau contabile, nu intră însă în domeniul de aplicare al Regulamentului general privind protecția datelor. Nici datele fără caracter personal, adică datele care nu sunt legate de o persoană fizică identificată sau identificabilă¹³, nu intră în domeniul de aplicare al Regulamentului general privind protecția datelor. Poate fi vorba, de exemplu, de date generate de calculatoare care nu au caracter personal.

Restricțiile referitoare la locul datelor pot izvorî din norme juridice sau orientări și practici administrative conform cărora stocarea sau prelucrarea datelor¹⁴ în format electronic¹⁵ trebuie să se limiteze la o anumită zonă geografică sau jurisdicție. Uneori, statele membre impun restricții în ideea că autoritățile de supraveghere pot să verifice mai ușor datele stocate la nivel local. Localizarea este utilizată, de asemenea, pe post de asigurare în ceea ce privește protecția vieții private, auditul și aplicarea legii, precum și securitatea datelor. În practică însă, aceste măsuri contribuie rareori la obiectivele pe care sunt menite să le atingă.

Securitatea informațiilor depinde de o serie de alți factori în afară de locul unde datele sunt stocate fizic, precum păstrarea confidențialității și a integrității acestor date atunci când ele sunt disponibile în afara centrului de stocare. În această privință, nu restricțiile referitoare la locul datelor, ci mai degrabă cele mai moderne procedee testate de gestionare în domeniul TIC, aplicate la o scară mult mai mare decât sistemele individuale, sunt cele care permit cu adevărat ca datele să fie stocate și prelucrate în securitate. De exemplu, pentru a păzi datele de catastrofe naturale sau atacuri cibernetice locale, centrele de stocare a datelor amplasate în diferite state membre ar putea să își salveze copii de rezervă unele în altele și să recurgă la măsurile tehnice și organizatorice prevăzute în Directiva privind securitatea rețelelor și a informațiilor¹⁶. De asemenea,

¹² Articolul 1 alineatul (3). De exemplu, o adresă IP dinamică înregistrată de un furnizor de servicii de comunicații electronice cu ocazia consultării de către o persoană a unui site internet pe care acest furnizor îl pune la dispoziția publicului constituie, pentru furnizorul respectiv, o dată cu caracter personal, în cazul în care acesta dispune de mijloace legale care îi permit să identifice persoana vizată cu ajutorul informațiilor suplimentare de care dispune furnizorul de acces la internet al acestei persoane. A se vedea hotărârea din cauza C-582/14, Breyer, ECLI:EU:C:2016:779, punctul 49.

¹³ Conform definiției de la articolul 4 alineatul (1) din Regulamentul general privind protecția datelor.

¹⁴ Atât date private, cât și date publice.

¹⁵ Inclusiv copii ale seturilor de date.

¹⁶ Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, JO L 194, 19.7.2016, p. 1.

disponibilitatea datelor pentru scopuri de reglementare sau de supraveghere, care nu este pusă în discuție în niciun fel, ar fi mai bine asigurată dacă s-ar îmbunătăți cooperarea dintre diferitele autorități naționale sau dintre autoritățile naționale și sectorul privat, decât dacă s-ar impune restricții de localizare. De fapt, în domeniile caracterizate de o cooperare strânsă între autoritățile de supraveghere, cum ar fi serviciile financiare, cerințele referitoare la localizarea datelor s-ar putea dovedi contraproductive¹⁷.

Cu toate acestea, în anumite contexte sau în legătură cu anumite date, în special înainte de introducerea unor modalități de cooperare transfrontalieră efectivă, anumite cerințe referitoare la localizarea datelor pot fi justificate și proporționale, cum ar fi tratarea securizată a anumitor date referitoare la infrastructura energetică critică sau punerea dovezilor electronice (de exemplu, copii localizate ale seturilor de date) la dispoziția autorităților de aplicare a legii sau stocarea locală a datelor păstrate în anumite registre publice.

Din nefericire, atât la nivel mondial, cât și în Europa se tinde tot mai mult spre localizarea datelor, o abordare bazată deseori pe ideea greșită că serviciile localizate sunt automat mai sigure decât serviciile transfrontaliere. În plus, piața serviciilor de date este în mare măsură influențată de lipsa unor reguli transparente și de puternica impresie că este nevoie ca datele să fie localizate. Se poate ajunge astfel la situații precum îngrădirea accesului întreprinderilor și al organizațiilor din sectorul public la servicii de date mai ieftine sau mai inovatoare sau obligarea întreprinderilor care își desfășoară activitatea la nivel transfrontalier să își creeze capacități suplimentare de stocare și de prelucrare a datelor. S-ar putea, de asemenea, ca, în acest fel, întreprinderile care exploatează date, în special start-up-uri și IMM-uri, să fie stânjenite în eforturile lor de a-și intensifica activitățile, de a pătrunde pe noi piețe (pentru că, de exemplu, ar trebui să investească în centre de date din 28 de state membre) sau de a-și centraliza capacitățile de date și cercetare analitică, în vederea dezvoltării de noi produse și servicii.

În prezent, cererea finală de servicii legate de TIC (consultanță, găzduire, dezvoltare) din Europa este satisfăcută intern, în interiorul UE, în proporție de 84 %. Dacă aceste servicii ar putea să se desfășoare cu mai multă ușurință și la nivel transfrontalier în cadrul UE, prin eliminarea restricțiilor referitoare la localizarea datelor, s-ar putea obține creșteri ale PIB-ului de până la 8 miliarde EUR, prin reduceri de costuri și sporuri de eficiență¹⁸.

Localizarea datelor împiedică, de asemenea, adoptarea pe scară mai largă a tehnologiei de stocare și informatică în cloud, ceea ce ar putea avea și efecte mai ample asupra societății. De fapt, utilizarea mai eficientă a resurselor informatice ar putea contribui la reducerea netă, cu cel puțin 30 %, a consumului de energie și a emisiilor de dioxid de carbon. O întreprindere de mici dimensiuni care folosește cloud-ul și-ar putea reduce consumul de energie și emisiile de dioxid de carbon cu peste 90 %, dacă își mută aplicațiile din infrastructura proprie în cloud. Se preconizează că piața mondială a

¹⁷ În conformitate cu numeroase dispoziții ale UE referitoare la serviciile financiare și cu Sistemul european de supraveghere financiară, autoritățile de supraveghere trebuie să aibă acces la date despre instituțiile și tranzacțiile financiare de pe întreg teritoriul UE. Cerințele ca datele să fie stocate pe un anumit teritoriu național sau condiționarea accesului autorităților de supraveghere la procedurile administrative ar putea restrânge accesul autorităților de supraveghere la date care le sunt indispensabile pentru îndeplinirea misiunii lor.

¹⁸ „Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States”, ECIPE, 2016, calcul bazat pe creșterea presiunii concurențiale în cadrul unei piețe unice digitale „industriale” în care prețurile sunt complet transparente.

centrelor de date eficiente din punct de vedere energetic va crește la aproximativ 90 de miliarde EUR până la sfârșitul anului 2020. Fragmentarea pieței serviciilor de date ar putea afecta dezvoltarea deplină a acestor servicii caracterizate de o utilizare mai eficientă a energiei în UE și, de asemenea, voința de a investi.

Pentru ca problemele și restricțiile menționate mai sus să poată fi ținute sub control și pentru ca economia europeană a datelor să își poată realiza pe deplin potențialul, statele membre ar trebui să se ghideze, în toate acțiunile pe care le întreprind și care influențează stocarea sau prelucrarea datelor, după „**principiul liberei circulații a datelor în UE**”, o consecință logică a obligațiilor care le revin în temeiul dispozițiilor referitoare la libera circulație a serviciilor și la libertatea de stabilire din tratat și în temeiul legislației secundare relevante. Fiecare restricție existentă sau nouă referitoare la locul datelor trebuie să fie justificată cu grijă în temeiul tratatului și al legislației secundare relevante, pentru a se asigura că este necesară și proporțională pentru atingerea unui obiectiv imperativ de interes general, cum este cel al securității publice¹⁹.

Principiul liberei circulații a datelor cu caracter personal²⁰, consacrat în legislația primară și în legislația secundară, ar trebui să se aplice și în cazurile în care Regulamentul general privind protecția datelor permite statelor membre să reglementeze aspecte specifice. Statele membre ar trebui încurajate să nu recurgă la derogările prevăzute în Regulamentul general privind protecția datelor pentru a restricționa și mai mult fluxul liber al datelor.

În concluziile sale din 15 decembrie 2016, Consiliul European a solicitat înlăturarea obstacolelor rămase în cadrul pieței unice, inclusiv a acelor care împiedică libera circulație a datelor²¹.

Pentru punerea în practică a principiului liberei circulații a datelor, Comisia va proceda în două etape, după cum urmează:

- după publicarea prezentei comunicări, Comisia va începe dialoguri structurate cu statele membre și alte părți interesate pe tema justificării și a proporționalității măsurilor referitoare la locul datelor, pornind de la restricțiile pe care le-a identificat până în prezent;
- după ce va cunoaște rezultatele dialogurilor și după ce va aduna – în cadrul consultării publice aferente, printre altele – noi informații despre dimensiunea și natura restricțiilor referitoare la locul datelor și despre efectele acestor restricții,

¹⁹ Ținându-se seama de faptul că excepțiile prevăzute în tratat trebuie să fie interpretate în mod restrictiv. Din legislația secundară relevantă în acest caz fac parte Regulamentul general privind protecția datelor, Directiva 2000/31/CE (Directiva privind comerțul electronic), Directiva 2006/123/CE (Directiva privind serviciile) și, în ceea ce privește proiectele de reglementări tehnice și proiectele de norme pentru serviciile societății informaționale, Directiva 2015/1535 (Directiva privind transparența).

²⁰ Libera circulație a datelor cu caracter personal este prevăzută la articolul 16 din Tratatul privind funcționarea Uniunii Europene, iar normele pentru libera circulație a datelor cu caracter personal sunt prevăzute în legislația actuală și viitoare a UE în materie de protecție a datelor. La articolul 1 alineatul (3) din Regulamentul general privind protecția datelor se prevede: „Libera circulație a datelor cu caracter personal în interiorul Uniunii nu poate fi restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.”

²¹ <http://www.consilium.europa.eu/eu/en/press-releases/2016/12/15-euro-conclusions-final/>

cu precădere asupra IMM-urilor și a start-up-urilor, Comisia va introduce, când este necesar, acțiuni în constatarea neîndeplinirii obligațiilor pentru înlăturarea măsurilor nejustificate sau disproporționate referitoare la locul datelor, putând de asemenea, dacă este necesar, să adopte noi inițiative privind fluxul liber al datelor. Toate acțiunile întreprinse ulterior în acest context vor respecta principiile unei mai bune legiferări.

3. ACCESUL LA DATE ȘI TRANSFERUL DE DATE

Calculatoarele și procesele care au la bază tehnologii emergente, cum ar fi internetul obiectelor, generează volume tot mai mari de date. Aceste date reprezintă o componentă esențială utilizată tot mai des în serviciile noi, inovatoare, în scopul îmbunătățirii produselor sau al proceselor de producție și în scopul sprijinirii procesului decizional.

Diversitatea datelor generate de aceste calculatoare sau procese prezintă pentru actorii de pe piața datelor posibilități variate de inovare și de aplicare a observațiilor făcute pe baza respectivelor date. De exemplu, datele culese cu ajutorul senzorilor utilizați în fermele moderne ar putea fi utilizate la crearea unei aplicații de optimizare a recoltelor, iar datele generate de senzorii din semafoare ar putea fi utilizate la crearea unei aplicații de gestionare a traficului sau de optimizare a traseului.

Pentru a extrage valoarea maximă din acest tip de date, actorii pieței trebuie să aibă acces la seturi de date mari și diversificate. Acest lucru va fi însă tot mai greu de realizat, dacă datele sunt păstrate de generatorii lor și sunt apoi analizate în izolare. Accesul la datele primare (adică date care nu au suferit nicio prelucrare și nicio modificare din momentul înregistrării lor) generate de aceste calculatoare sau procese și transferul acestor date sunt, prin urmare, aspecte esențiale pentru crearea unei economii a datelor și necesită o analiză atentă.

Aspectul accesului la datele generate de calculatoare este examinat în prezent în mai multe sectoare, cum ar fi transporturile, piețele energiei, mediile de locuit inteligente și sectorul serviciilor de sănătate și de îngrijire.

Înainte de a se analiza situația actuală a accesului la date în UE, este important să se precizeze clar tipul de date avute în vedere în acest context.

3.1. Tipul de date avute în vedere

În general, datele se împart în date cu caracter personal și date fără caracter personal. De exemplu, datele generate de senzorii de temperatură dintr-o locuință pot avea un caracter personal dacă pot fi puse în legătură cu o persoană în viață, în timp ce datele referitoare la umiditatea solului nu au caracter personal. Datele cu caracter personal pot fi transformate în date fără caracter personal prin procesul de anonimizare. Dacă se consideră că datele au caracter personal²², se aplică cadrul de protecție a datelor, în special Regulamentul general privind protecția datelor.

²² Conform definiției de la articolul 4 alineatul (1) din Regulamentul general privind protecția datelor.

Datele generate de calculatoare sunt create fără intervenția directă a omului, prin intermediul unor procese, aplicații sau servicii informatice sau prin intermediul unor senzori care prelucrează informațiile primite de la echipamente, software-uri sau aparate reale sau virtuale.

Datele generate de calculatoare pot fi date cu caracter personal sau date fără caracter personal. Dacă datele generate de calculatoare permit identificarea unei persoane fizice (cum ar fi datele de localizare din aplicațiile mobile), se consideră că datele respective au caracter personal, consecința fiind că până la anonimizarea deplină a acestora se aplică toate normele privind datele cu caracter personal.

O temă care privește atât fluxul liber de date, cât și întrebările nou apărute în legătură cu accesul la date și transferul de date este aceea că întreprinderile și actorii din economia datelor se vor ocupa atât cu date cu caracter personal, cât și cu date fără caracter personal, și că fluxurile și seturile de date vor conține cu regularitate ambele tipuri de date. La adoptarea oricărei măsuri de politică trebuie să se țină seama de această realitate economică și de cadrul juridic în materie de protecție a datelor cu caracter personal, respectându-se în același timp drepturile fundamentale ale persoanelor.

3.2. Limitarea accesului la date

Pentru examinarea acestei întrebări nou apărute, trebuie să se analizeze mai întâi modul în care întreprinderile și alți actori ai pieței pot avea acces la seturile de date mari și diversificate care sunt necesare în economia datelor.

Din informațiile disponibile²³ rezultă că întreprinderile care dețin cantități mari de date tind, în general, să utilizeze în principal capacitățile proprii de cercetare analitică a datelor. În majoritatea cazurilor, datele sunt generate și analizate de aceeași întreprindere, fiind posibil să nu fie reutilizate ulterior, chiar dacă întreprinderea subcontractează sarcina de analizare a respectivelor date. De altfel, se întâmplă uneori ca fabricanții, furnizorii de servicii sau alți actori ai pieței care dețin date să păstreze pentru ei datele generate de calculatoarele lor sau prin produsele și serviciile lor, putând astfel să limiteze reutilizarea respectivelor date pe piețele din aval. Multe întreprinderi fie nu profită de posibilitatea de a utiliza interfețe de programare a aplicațiilor (API-uri) ușor de folosit²⁴, fie nu permit utilizarea acestora; aceste interfețe arată modul în care ar trebuie să interacționeze diferitele aplicații și pot servi ca porturi de intrare sigure pentru utilizările noi și inovatoare ale datelor deținute de întreprinderi.

În ansamblu, schimbul de date continuă, așadar, să fie limitat. Piețele de date apar puțin câte puțin, dar nu sunt utilizate pe scară largă. S-ar putea ca întreprinderile să nu dispună de instrumentele și competențele potrivite pentru cuantificarea valorii economice a datelor lor și să se teamă că își vor pierde sau compromite avantajul concurențial dacă întreprinderile concurente obțin accesul la respectivele date.

²³ IDC, European Data Market Study, Primul raport intermediar, 2016; Impact Assessment support study on emerging issues of data ownership, interoperability, (re)usability and access to data, and liability, Primul raport intermediar, 2016; DG CONNECT Conferința la nivel înalt, 17 octombrie 2016.

²⁴ De exemplu, <https://developer.lufthansa.com/>; <https://data.sncf.com/api>; <https://api.tfl.gov.uk/>; <https://dev.blablacar.com/>.

3.3. Datele primare generate de calculatoare: situația juridică la nivelul UE și la nivel național

Datele primare generate de calculatoare nu sunt protejate prin drepturile de proprietate intelectuală existente, întrucât nu se consideră că ele ar fi rezultatul vreunui efort intelectual și/sau că ar avea vreun grad de originalitate. Dreptul *sui generis* din Directiva privind bazele de date (96/9/CE) – dreptul producătorilor de baze de date de a interzice extragerea și/sau reutilizarea ansamblului sau a unei părți substanțiale a conținutului unei baze de date – poate oferi protecție numai în condițiile în care pentru crearea unei baze de date sunt necesare investiții substanțiale pentru obținerea, verificarea sau prezentarea conținutului său. Directiva privind protecția secretelor comerciale (2016/943/UE), care a fost adoptată de curând și care trebuie transpusă în dreptul intern până în iunie 2018, va asigura protecția secretelor comerciale împotriva dobândirii, utilizării și divulgării ilegale. Pentru ca datele să fie considerate „secret comercial”, trebuie să se ia măsuri de păstrare a confidențialității informațiilor care constituie „capitalul intelectual al întreprinderii”.

În temeiul dreptului aplicabil în diferitele state membre, datele pot face obiectul unor acțiuni în justiție numai atunci când îndeplinesc anumite condiții pentru a fi considerate, de exemplu, proprietate intelectuală, bază de date sau secret comercial. În general, datele primare generate de calculatoare nu îndeplinesc însă în sine condițiile relevante la nivelul UE.

Prin urmare, în prezent nu există cadre cuprinzătoare de politică nici la nivel național, nici la nivelul Uniunii – nici în ceea ce privește datele primare generate de calculatoare care nu pot fi considerate date cu caracter personal, nici în ceea ce privește condițiile pentru exploatarea economică și posibilitatea de comercializare a respectivelor date. Problema este rezolvată de cele mai multe ori prin intermediul contractelor. Utilizarea instrumentelor existente de drept general al contractelor și de drept al concurenței, care sunt disponibile în Uniune, ar putea constitui o soluție suficientă. În plus, ar putea fi avute în vedere acorduri voluntare sau acorduri-cadru sectoriale. S-ar putea însă ca, atunci când diferiții participanți la piață nu au aceeași putere de negociere, soluțiile bazate pe piață să nu fie suficiente pentru asigurarea unor rezultate corecte și favorabile inovării, pentru facilitarea accesului nou-veniților pe piață și pentru evitarea situațiilor de client captiv.

3.4. Situația în practică

În anumite cazuri, fabricanții sau furnizorii de servicii pot deveni *de facto* „proprietari” ai datelor generate de calculatoarele sau procesele lor, chiar dacă respectivele calculatoare se află în proprietatea utilizatorului. Un control *de facto* asupra acestor date poate constitui pentru fabricanți o sursă de diferențiere și de avantaje concurențiale. Această situație poate fi însă problematică, deoarece utilizatorii sunt deseori împiedicați de fabricanți să autorizeze utilizarea datelor de către o altă parte.

Diferiții actori ai pieței care dețin controlul asupra datelor ar putea astfel, în funcție de specificul piețelor, să profite de lacunele cadrului de reglementare sau de insecuritățile juridice descrise mai sus și să le impună utilizatorilor clauze abuzive în contractele standard sau să recurgă la mijloace tehnice precum formate sau criptări protejate prin drepturi exclusive. Referitor la clauzele contractuale abuzive, tranzacțiile dintre întreprinderi, B2B, au fost incluse în domeniul de aplicare al Directivei privind drepturile

consumatorilor în câteva state membre, dar nu în toate. Rezultatul acestei situații ar putea fi, de exemplu, ca utilizatorii și întreprinderile să se regăsească captivi în contracte exclusive de exploatare a datelor. Este posibil să se ajungă la un schimb voluntar de date, dar negocierea unor contracte de acest fel ar putea presupune costuri de tranzacție considerabile pentru părțile mai slabe, atunci când negocierea nu se face pe picior de egalitate sau când costurile de consultanță juridică sunt semnificative.

3.5. Un viitor cadru al UE pentru accesul la date

Câteva state membre examinează în prezent posibilitatea de a asigura accesul la datele generate de calculatoare și ar putea hotărî să reglementeze singure această chestiune. O abordare necoordonată ascunde riscul unei fragmentări și ar dăuna atât eforturilor de dezvoltare a unei economii a datelor la nivelul UE, cât și funcționării serviciilor și tehnologiilor transfrontaliere de date pe piața internă.

De aceea, Comisia intenționează să poarte un dialog cu statele membre și cu alte părți interesate, în cadrul căruia să analizeze posibilitatea unui viitor cadru al UE pentru accesul la date. Comisia consideră că acest dialog ar trebui să se învârtă în jurul celor mai eficiente modalități de îndeplinire a următoarele obiective:

- **îmbunătățirea accesului la datele anonime generate de calculatoare** – prin faptul că sunt partajate, reutilizate și agregate, datele generate de calculatoare creează valoare, devin o sursă de inovare și permit diversificarea modelelor de afaceri²⁵;
- **facilitarea și stimularea partajării acestor date** – în soluțiile viitoare, oricare ar fi ele, ar trebui să se promoveze accesul efectiv la date, ținându-se seama, de exemplu, de posibilele diferențe dintre actorii pieței în ceea ce privește puterea de negociere;
- **protejarea investițiilor și a activelor** – în soluțiile viitoare, oricare ar fi ele, ar trebui să se țină seama, de asemenea, de interesele legitime ale actorilor pieței care investesc în dezvoltarea de produse, să se asigure o rentabilitate echitabilă a investițiilor lor și să se contribuie astfel la inovare. În același timp, în soluțiile viitoare, oricare ar fi ele, ar trebui să se asigure o repartizare echitabilă a beneficiilor între deținătorii de date²⁶, persoanele împuternicite de către operatori și furnizorii de aplicații din cadrul lanțurilor valorice;
- **evitarea divulgării datelor confidențiale** – prin soluțiile viitoare, oricare ar fi ele, ar trebui să se reducă riscurile de divulgare a datelor confidențiale, în special față de concurenții existenți sau potențiali. În această privință, ar trebui să se poată efectua, de asemenea, o clasificare corespunzătoare a datelor înainte de a se verifica dacă o anumită dată poate fi partajată sau nu;
- **reducerea la minimum a efectelor de client captiv** – ar trebui să se țină seama de faptul că întreprinderile și persoanele fizice nu au aceeași putere de negociere.

²⁵ Când este vorba de date cu caracter personal, se aplică Regulamentul general privind protecția datelor.

²⁶ Entitatea care gestionează și păstrează datele generate de calculatoare în practică.

Ar trebui evitate situațiile de client captiv, în special în cazul IMM-urilor, al start-up-urilor și al persoanelor fizice.

În dialogurile cu părțile interesate, Comisia intenționează să discute următoarele posibilități de abordare a accesului la datele generate de calculatoare, care diferă în funcție de nivelul de intervenție:

- **orientări pentru motivarea întreprinderilor să partajeze informații** – pentru atenuarea efectelor produse de diferențele dintre reglementările naționale și pentru a oferi întreprinderilor mai multă securitate juridică, Comisia ar putea emite orientări cu privire la modul în care ar trebui abordate în contracte drepturile de control asupra datelor fără caracter personal. Aceste orientări ar urma să se bazeze pe legislația existentă, mai precis pe cerințele de transparență și echitate prevăzute în dreptul UE în materie de marketing și consumatori, Directiva privind secretele comerciale și legislația în materie de drepturi de autor, în special Directiva privind bazele de date. Comisia intenționează să lanseze o evaluare a Directivei privind bazele de date în 2017.
- **încurajarea dezvoltării de soluții tehnice pentru identificarea fiabilă a datelor și schimbul fiabil de date** – controlul real al datelor de pe piață poate avea loc numai dacă sursele de date sunt trasabile și clar identificate. Pentru a se crea încredere în sistem, ar putea fi necesar să se stabilească protocoale fiabile și eventual standardizate de identificare continuă a surselor de date. Interfețele de programare a aplicațiilor (API-uri) pot promova, la rândul lor, crearea unui ecosistem alcătuit din dezvoltatori de aplicații și de algoritmi care sunt interesați de datele deținute de întreprinderi. API-urile pot ajuta întreprinderile și autoritățile publice să găsească diferite modalități de reutilizare a datelor pe care le dețin și să profite de respectivele modalități. În acest context s-ar putea avea în vedere, pe baza unor orientări tehnice, utilizarea pe o scară mai largă a unor API-uri cu sursă deschisă („open source”) care să fie standardizate și bine documentate, inclusiv identificarea bunelor practici și difuzarea acestora către întreprinderi și organisme din sectorul public. Aici ar putea intra și punerea la dispoziție a datelor în formate citibile automat și furnizarea metadatelor asociate;
- **stabilirea unor reguli standard pentru contracte** – regulile standard ar putea constitui o soluție de referință echilibrată pentru contractele legate de date, iar la stabilirea lor ar trebui să se țină seama în mod corespunzător și de rezultatele verificării adecvării la care este supusă în prezent Directiva privind clauzele contractuale abuzive. Simultan cu aceste reguli standard ar putea fi introdus un control al caracterului abuziv din relațiile contractuale B2B²⁷, care să atragă invalidarea clauzelor contractuale care se abat excesiv de la regulile standard. Aceste reguli ar putea fi completate, de asemenea, cu un set de clauze contractuale standard recomandate, concepute de părțile interesate. Prin această abordare s-ar putea diminua atât obstacolele juridice de care se lovesc întreprinderile mici, cât și dezechilibrul pozițiilor de negociere, permițându-se în continuare un grad ridicat de libertate contractuală;

²⁷. Desigur că ce se consideră abuziv în contractele dintre întreprinderi, B2B, ar trebui să fie diferit de ce se consideră abuziv în contractele dintre întreprinderi și consumatori, B2C, astfel încât să fie pus în evidență faptul că în relațiile B2B există un grad mai mare de libertate contractuală.

- **accesul la date în interes public și în scopuri științifice** – autorităților publice li s-ar putea acorda accesul la date când acest acces ar fi în „interesul general” și ar îmbunătăți considerabil funcționarea sectorului public; este vorba, de exemplu, de accesul oficiilor de statistică la date comerciale sau de optimizarea sistemelor de gestionare a traficului pe baza unor date obținute în timp real de la autovehicule private. Accesul autorităților de statistică la datele comerciale ar contribui, în mod normal, la reducerea costului suportat de agenții economici pentru îndeplinirea obligațiilor de raportare statistică. De asemenea, accesul la date din diferite surse și posibilitatea de a combina aceste date sunt esențiale pentru cercetarea științifică în domenii precum științele medicale, științele sociale și științele de mediu;
- **drepturile producătorului de date** – „producătorul de date”, și anume proprietarul sau utilizatorul pe termen lung, adică posesorul dispozitivului ar putea beneficia de dreptul de a utiliza date fără caracter personal și de dreptul de a autoriza utilizarea acestora. Scopul acestei abordări este ca situația juridică a producătorului de date să fie clară și ca respectivul producător să dispună de o mai mare libertate de decizie, prin faptul că utilizatorilor li se oferă posibilitatea de a-și utiliza datele și de a contribui astfel la deblocarea datelor generate de calculatoare. Ar trebui totuși să se precizeze clar care sunt excepțiile relevante, în special acordarea accesului neexclusiv la date de către fabricant sau de către autoritățile publice, de exemplu pentru gestionarea traficului sau din motive de mediu. Când este vorba de date cu caracter personal, persoana își va păstra dreptul de a-și retrage consimțământul în orice moment după autorizarea utilizării. Datele cu caracter personal ar trebui să fie anonimizate, astfel încât persoana să nu fie sau să nu mai fie identificabilă, înainte ca cealaltă parte să autorizeze o nouă utilizare a lor. De fapt, Regulamentul general privind protecția datelor continuă să se aplice tuturor datelor cu caracter personal (indiferent dacă sunt generate de calculatoare sau în alt mod) până în momentul anonimizării acestora;
- **accesul contra cost** – pentru deținătorii de date, cum ar fi fabricanții, furnizorii de servicii sau alte părți, s-ar putea elabora un cadru care să se bazeze eventual pe anumite principii esențiale, cum ar fi principiul unor clauze echitabile, rezonabile și nediscriminatorii (FRAND), și prin care deținătorii de date să ofere contra cost accesul la datele pe care le dețin, după anonimizarea acestora. Ar trebui să fie luate în considerare atât interesele legitime relevante, cât și nevoia de protejare a secretelor comerciale. Pentru a se ține seama de specificul fiecărui sector, s-ar putea avea în vedere stabilirea unor regimuri de acces separate pentru diferitele sectoare și/sau modele de afaceri. De exemplu, accesul liber la date (total sau parțial) ar putea fi, în unele cazuri, opțiunea preferată atât pentru întreprinderi, cât și pentru societate.

Comisia va consulta părțile interesate în chestiunile descrise mai sus, pentru a aduna mai multe informații referitoare la funcționarea piețelor de date în funcție de sector și pentru a analiza posibilele soluții. În acest context, o dezbatere amplă la nivel macroeconomic este esențială pentru discutarea unor posibile soluții și pentru evitarea efectelor colaterale neintenționate care ar putea frâna inovația sau concurența. Vor avea loc, de asemenea, discuții sectoriale cu părțile interesate relevante din lanțul valoric al datelor.

4. RĂSPUNDEREA

O altă temă care se profilează este aplicarea normelor actuale de răspundere în economia datelor în ceea ce privește produsele și serviciile bazate pe tehnologiile emergente, cum ar fi internetul obiectelor, fabricile viitorului și sistemele autonome conectate. Internetul obiectelor este o rețea în rapidă creștere de obiecte de uz cotidian, cum ar fi ceasurile de mână, autovehiculele și termostatele care sunt conectate la internet. Sistemele autonome conectate, cum ar fi autovehiculele autonome, acționează independent de om și au capacitatea de a înțelege și a interpreta mediile în care acționează. Aceste tehnologii emergente furnizează, cu ajutorul senzorilor din dotare, numeroasele tipuri de date de care produsul sau serviciul în cauză are deseori nevoie pentru a funcționa.

Deși toate aceste inovații sunt menite să mărească siguranța și calitatea vieții, în cazul niciunui dispozitiv nu se poate exclude posibilitatea erorilor de proiectare, a avariilor sau a manipulărilor. Aceste defecte ar putea rezulta din transmiterea unor date eronate de către senzori, ca urmare, de exemplu, a unor defecte de software, a unor probleme de conexiune sau a funcționării incorecte a calculatorului. Dată fiind natura acestor sisteme, ar putea fi dificil să se stabilească cu exactitate sursa problemei care produce prejudicii, născându-se astfel două întrebări: cum s-ar putea garanta că aceste sisteme sunt sigure pentru utilizatori, în vederea reducerii la minimum a producerii de prejudicii, și cine răspunde pentru prejudiciile produse.

De o importanță majoră pentru apariția unei economii a datelor este, prin urmare, modul în care se poate oferi securitate atât utilizatorilor, cât și producătorilor de dispozitive, în legătură cu posibila lor răspundere.

4.1. Normele UE în materie de răspundere

În dreptul civil se face, în general, distincția între două tipuri de răspundere juridică: răspunderea contractuală, când răspunderea pentru prejudiciul creat rezultă din relația contractuală existentă între părți, și răspunderea extracontractuală²⁸, când aspectele răspunderii sunt reglate în afara unui contract. Un tip important de răspundere extracontractuală este răspunderea pentru produsele cu defect. La nivelul UE, în Directiva privind răspunderea pentru produsele cu defect (85/374/CEE) („Directiva privind răspunderea pentru produse”) este stabilit principiul răspunderii obiective, adică al răspunderii fără culpă: dacă un produs cu defect cauzează prejudicii consumatorului, este posibil ca fabricanții să răspundă pentru respectivele prejudicii, chiar dacă acestea nu s-au produs din neglijența sau culpa lor. Cu toate acestea, modul în care se aplică dispozițiile directivei²⁹ menționate în contextul internetului obiectelor și al sistemelor autonome conectate (de exemplu, robotica) ar putea fi dificil de stabilit sau ar putea fi neclar din următoarele motive: caracteristicile acestor sisteme – cum ar fi natura complicată a lanțului valoric al produsului sau al serviciului, caracterizat de interdependențe între furnizori, fabricanți și alte părți terțe –, insecuritatea existentă în legătură cu natura juridică a dispozitivelor din domeniul internetului obiectelor – adică

²⁸ Normele UE în materie de răspundere se referă doar la răspunderea extracontractuală.

²⁹ Răspunderea obiectivă pe care o poartă producătorii în cazul produselor cu defect este amintită și în alte acte normative referitoare la siguranța produselor, cum ar fi Directiva privind echipamentele radio (2014/53/UE), regulamentele privind dispozitivele medicale, Directiva privind echipamentele tehnice (2006/42/CE) și Directiva privind siguranța generală a produselor (2001/95/CE).

dacă este vorba de produse, de servicii sau de produse achiziționate împreună cu un serviciu – și natura autonomă a acestor tehnologii.

Comisia a lansat o amplă evaluare a Directivei privind răspunderea pentru produse, pentru a stabili cum funcționează aceasta în general și dacă normele sale, elaborate pentru un mediu foarte diferit, continuă să fie potrivite pentru tehnologiile emergente, cum ar fi internetul obiectelor și sistemele autonome conectate.

4.2. Posibile abordări pentru viitor

Obiectivul Comisiei este să consolideze securitatea juridică în ceea ce privește răspunderea în contextul tehnologiilor emergente și, astfel, să creeze condiții favorabile pentru inovare. În afară de statu-quo³⁰, ar putea fi analizate diferite abordări, cum ar fi:

- **abordarea bazată pe generarea riscului sau abordarea bazată pe gestionarea riscului** – în cadrul acestor abordări, răspunderea ar putea fi atribuită acelor actori ai pieței care generează un risc major pentru alții sau acelor care sunt cel mai bine plasați pentru a reduce la minimum sau pentru a evita materializarea riscului respectiv;
- **sistemele de asigurări obligatorii sau voluntare** – aceste sisteme ar putea fi combinate cu abordările de răspundere menționate mai sus. Ele ar compensa părțile care au suferit prejudicii (de exemplu, consumatorul). Prin această abordare ar trebui să se asigure protecția juridică a investițiilor efectuate de întreprinderi și, în același timp, să li se ofere asigurări victimelor că vor primi o compensație echitabilă sau o asigurare adecvată în caz de prejudicii.

Oricare ar fi abordarea aleasă, ar trebui să se țină seama de acțiunile persoanei care utilizează tehnologia și să se stabilească mai clar care ar trebui să fie rolul utilizatorilor tehnologiei respective.

Comisia va consulta părțile interesate pentru a stabili dacă normele actuale ale UE în materie de răspundere sunt adecvate în contextul internetului obiectelor și al sistemelor autonome conectate și care sunt abordările posibile pentru depășirea actualelor dificultăți legate de atribuirea răspunderii. În paralel se desfășoară, de asemenea, o consultare publică referitoare la evaluarea generală a aplicării Directivei privind răspunderea pentru produse. Comisia va evalua rezultatele și va analiza opțiunile de acțiuni viitoare.

5. PORTABILITATEA, INTEROPERABILITATEA ȘI STANDARDELE

Alte teme care se profilează în economia datelor sunt portabilitatea datelor fără caracter personal, interoperabilitatea serviciilor, necesară pentru schimbul de date, și standardele tehnice corespunzătoare pentru asigurarea unei portabilități efective.

³⁰ Comisia ar putea emite orientări privind aplicarea normelor UE în materie de răspundere în cazul internetului obiectelor și în cazul roboticii.

5.1. Portabilitatea datelor fără caracter personal

Portabilitatea datelor înseamnă că atât consumatorii, cât și întreprinderile își pot lua ușor datele dintr-un sistem în altul. În general, portabilitatea înseamnă costuri scăzute de trecere de la un sistem la altul și, astfel, un nivel scăzut de bariere la intrarea în economia datelor. În temeiul Regulamentului general privind protecția datelor, persoanele fizice vor avea dreptul de a primi, într-un format uzual structurat și citibil automat, datele cu caracter personal furnizate către prestatorul de servicii și dreptul de a transmite aceste date către un alt furnizor³¹.

În ceea ce privește însă datele fără caracter personal, în prezent nu există obligații de a garanta fie și un nivel minim de portabilitate a datelor nici măcar în cazul serviciilor online utilizate pe scară largă, cum ar fi găzduirea în cloud. Această situație se datorează în parte faptului că cerințele pentru asigurarea portabilității datelor pot fi solicitante din punct de vedere tehnic și costisitoare, dat fiind că este posibil ca diferiții furnizori ai aceluiași serviciu să stocheze datele în mod diferit.

La asigurarea portabilității efective a datelor fără caracter personal ar trebui să se țină seama, de asemenea, de aspectele mai largi ale guvernancei datelor, cum ar fi transparența pentru utilizatori, gestionarea accesului și interoperabilitatea necesară pentru a conecta între ele diferitele platforme într-un mod care să stimuleze inovarea.

5.2. Interoperabilitatea

Considerațiile de portabilitate a datelor sunt deseori strâns legate de chestiunea interoperabilității datelor, care permite, pe baza unor specificații tehnice corespunzătoare, schimbul fluid de date între mai multe servicii digitale. În Directiva privind informațiile din sectorul public și în orientările aferente (inclusiv Cadrul european de interoperabilitate) se subliniază importanța pe care metadatele concludente și standardizate, construite pe baza unui vocabular consacrat, o au în facilitarea căutării și a interoperabilității. Directiva de instituire a infrastructurii pentru informații spațiale în Comunitatea Europeană (Inspire), alături de regulamentele asociate în materie de interoperabilitate și orientările pentru serviciile de date spațiale și datele spațiale, inclusiv datele furnizate de senzori, se aplică în prezent pentru datele spațiale ale sectorului public³².

În cazul platformelor online, interoperabilitatea datelor facilitează nu doar trecerea de la o platformă la alta, ci și utilizarea simultană a mai multor platforme (conectarea simultană la mai multe rețele, așa-numitul „multi-homing”) și schimbul larg de date între diferite platforme, ceea ce are potențialul de a stimula inovarea în economia digitală.

³¹ Articolul 20.

³² Datele generate de calculatoare sunt „date spațiale”, întrucât, alături de măsurători, senzorii transmit, de obicei, și poziția lor directă sau indirectă (localizarea).

5.3. Standardele

Pentru a fi eficace și pentru a asigura portabilitatea efectivă într-un mod neutru din punct de vedere tehnologic, politicile adoptate în materie de portabilitate trebuie să se sprijine pe standarde tehnice corespunzătoare. Comisia s-a angajat³³ să sprijine standardele corespunzătoare în vederea îmbunătățirii interoperabilității, a portabilității și a securității serviciilor de cloud, prin integrarea mai pronunțată a activității comunităților „open source” în procesul de standardizare desfășurat la nivel european. Exemple pentru această abordare sunt specificațiile TOSCA pentru aplicațiile cloud, prin care se vizează îmbunătățirea portabilității și a managementului operațional al aplicațiilor și serviciilor cloud³⁴, și specificațiile și orientările tehnice din regulamentele de punere în aplicare a Directivei Inspire³⁵.

5.4. Posibile abordări pentru viitor

Printre abordările care ar putea fi adoptate în viitor pentru rezolvarea problemelor menționate mai sus se numără:

- **elaborarea unor clauze contractuale recomandate pentru facilitarea trecerii de la un furnizor de servicii la altul** – întrucât portabilitatea datelor și trecerea de la un furnizor de servicii de date la altul sunt interdependente, s-ar putea avea în vedere elaborarea unor clauze contractuale standard prin care furnizorul de servicii să fie obligat să asigure portabilitatea datelor clientului;
- **introducerea unor noi drepturi în domeniul portabilității datelor** – pornind de la dreptul la portabilitatea datelor prevăzut în Regulamentul general privind protecția datelor și de la propunerile de norme pentru contractele de furnizare a conținutului digital, ar putea fi introdus dreptul la portabilitatea datelor fără caracter personal, în special în contextele B2B, ținându-se seama totuși de rezultatul verificării adecvării la care sunt supuse în prezent câteva acte esențiale din dreptul UE în materie de marketing și de protecție a consumatorilor³⁶;
- **experimentarea sectorială a standardelor** – pentru crearea unei abordări solide a normelor de portabilitate codificate prin standarde, ar putea fi lansate metode experimentale sectoriale. Acestea ar trebui să presupună, în mod normal, colaborarea a mai multe părți interesate, printre care autoritățile de standardizare, reprezentanții sectorului, comunitatea tehnică și autoritățile publice.

Comisia va consulta părțile interesate cu privire la aceste chestiuni și va decide apoi dacă trebuie luate măsuri suplimentare, eventual sub forma măsurilor menționate mai sus, fie separat, fie combinat.

³³ COM(2016) 176 final: Priorități de standardizare în sectorul TIC pentru piața unică digitală.

³⁴ <https://www.oasis-open.org/committees/tosca>.

³⁵ Legislația Inspire: <http://inspire.ec.europa.eu/inspire-legislation/26>.

³⁶ http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm.

6. EXPERIMENTAREA ȘI TESTAREA

Experimentarea constituie o parte importantă din analiza temelor care se profilează în economia datelor. În acest sens se va cântări posibilitatea de a finanța aceste exerciții de probă și experimente prin Programul Orizont 2020.

Înainte de a se concluziona dacă o posibilă soluție de acces la date și de răspundere este potrivită sau nu, ar trebui organizat un exercițiu de probă, în cadrul căruia aceste probleme să fie testate într-un mediu real, în parteneriat cu părțile interesate. Este nevoie de o soluție europeană, fondată pe cooperarea statelor membre și pe efectuarea unor experimente comune.

Tema unui exercițiu de probă de acest fel ar putea fi mobilitatea cooperativă, conectată și automatizată³⁷, dată fiind dimensiunea transfrontalieră a acestui sector.

În mai multe state membre se desfășoară în prezent proiecte de creare a unor sisteme cooperative și de mărire a nivelurilor de automatizare³⁸. În cadrul acestor proiecte, autovehiculele se conectează unele cu altele și cu infrastructura rutieră – semafoare și indicatoare rutiere. Mai mult, Comisia intenționează să colaboreze cu un grup de state membre interesate și să creeze un cadru juridic pentru teste prin care să se poată efectua experimente pe baza unor norme armonizate pentru accesul la date și pentru răspundere. Pentru a permite accesul la un volum de date suficient de mare, exercițiile de probă ar trebui să fie efectuate cu tehnologie 5G, în coexistență armonioasă cu tehnologiile deja prezente și după principiul complementarității³⁹.

Un alt experiment interesant este oferit de sectorul geospațial, prin apariția unui nou ecosistem de date construit în jurul Copernicus, programul UE de observare a Pământului și al treilea cel mai mare furnizor de date din lume. Comisia se ocupă în prezent cu o serie de soluții inovatoare pentru stimularea dezvoltării de aplicații bazate pe Copernicus și alte date spațiale, încercând să rezolve în principal problema accesului la date, a interoperabilității și a previzibilității acestora.

7. CONCLUZIE

Pentru construirea economiei datelor, UE are nevoie de un cadru de politici în care datele să poată fi utilizate de-a lungul lanțului valoric în scopuri științifice, societale și industriale. În acest sens, Comisia lansează un amplu dialog cu părțile interesate pentru discutarea aspectelor analizate în prezenta comunicare. Prima etapă a acestui dialog va fi o consultare publică. Accesul la date și răspunderea vor fi, de asemenea, testate într-un mediu real în domeniul mobilității cooperative, conectate și automatizate.

Referitor la fluxul liber al datelor, Comisia va continua să trateze acest subiect în concordanță cu abordarea explicată mai sus, pentru ca principiul liberei circulații a datelor în UE să fie pe deplin aplicat, inclusiv, atunci când este necesar și indicat, prin

³⁷ A se vedea COM (2016) 766 din 30.11.2016.

³⁸ A se vedea COM(2016) 766: O strategie europeană privind sistemele de transport inteligente cooperative.

³⁹ A se vedea COM(2016) 588: Un plan de acțiune privind 5G în Europa.

intermediul unor măsuri prioritare de punere în aplicare. Comisia va continua, de asemenea, să monitorizeze fluxul liber al datelor și să adune informații și, dacă este necesar, ar putea avea în vedere noi inițiative în domeniul liberei circulații a datelor.

În funcție de rezultatele dialogului cu părțile interesate, Comisia va decide, de asemenea, dacă sunt necesare măsuri suplimentare în legătură cu problemele care se profilează și va propune soluții în consecință. În acest context, experimentarea în condiții reale ar putea avea un rol de jucat.