ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOM LXVIII/2, ŞTIINŢE JURIDICE, 2022

DOI: 10.47743/jss-2022-68-3-10

Internet of Things – Perspective europene asupra dreptului de acces la date

Internet of Things – European perspectives on data access rights

Alexandru Chistruga[1]

Rezumat: IoT (Internet-of-Things) sau internetul obiectelor reprezintă o reţea de obiecte *smart* (conectate la internet) în care sunt incorporate senzori electronici în scopul colectării şi schimbului de date cu alte dispozitive *smart*. În literatura de specialitate s-a pus problema privind persoana îndreptăţită să aibă acces la aceste date (fabricanţii senzorilor, fabricantul obiectului *smart*, proprietarul acestui obiect, furnizorul de conţinut digital, furnizorul de *cloud)*. În lucrarea *Iot-Perspective Europene asupra dreptului de acces la date* se va încerca clarificarea acestei probleme prin prisma reglementărilor europene actuale, dar şi a celor aflate în stadiul de propunere.

Cuvinte-cheie: Internetul obiectelor, dreptul de acces la date, Legea privind datele

Abstract: IoT (Internet of Things) is a network of smart objects that are embedded with electronic sensors that aim to collect and exchange data with other smart devices. The legal literature has raised the question of the person entitled to have access to data (sensor manufacturers, smart object manufacturer, owner of this object, digital content provider, cloud provider). The study *Iot-European Perspectives on Data Access Rights* will attempt to clarify this issue in light of current European regulations, as well as those in the proposal stage.

Keywords: Internet of Things, data access rights, Data Act

Aspecte introductive

Tehnologiile digitale sunt în continuă dezvoltare, fiind omniprezente în majoritatea domeniilor vieţii noastre, aducând numeroase beneficii, dar şi multe provocări în ceea ce priveşte securitatea informaţiilor pe care le oferim furnizorilor de produse şi servicii conexe.

O categorie de tehnologii digitale, care devine tot mai răspândită în ultimii ani, este reprezentată de IoT (*Internet of Things*). Deşi există impresia că IoT se limitează la obiectele *smart* de uz casnic, cum ar fi *IoT-Powered Multicookers, smart watches sau smart TV*, realitatea constă în aceea că orice dispozitiv care are abilitatea de a se conecta la internet pentru a comunica cu alte obiecte *smart* face parte din reţeaua IoT.

[1] Masterand, Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iași, e-mail: alexandruchistruga98@gmail.com

Pentru buna lor funcţionare, IoT colectează şi stochează o cantitate enormă de date cu caracter personal şi fără caracter personal. Spre exemplu, potrivit unui raport[2] prezentat de *Federal Trade Commision* din Statele Unite ale Americii, în anul 2015, 10.000 de gospodării casnice care utilizau dispozitive *smart* puteau genera peste 150 de milioane de date pe zi. Apreciem că această statistică este incidentă şi în cazul Uniunii Europene. În cele mai multe cazuri, utilizatorii îşi dau acordul pentru colectarea acestora fără a cunoaşte în ce scop vor fi folosite şi, prin urmare, necunoscând în ce condiţii au dreptul de acces la propriile date.

În vederea instituirii unui cadru legal în care să fie prevăzute norme care să reglementeze dreptul de acces la datele colectate de dispozitivele conexe atât de furnizorul de produs, cât şi de consumator, Comisia Europeană a elaborat două propuneri de Regulament în acest domeniu.

Astfel, prima propunere se referă la Legea privind guvernanţa datelor[3] (devenită Regulamentul 2022/868) care încearcă să abordeze „schimbul de date între întreprinderi, în schimbul unei remuneraţii sub orice formă”[4], iar a doua propunere, Legea privind datele[5], are drept obiective „facilitarea accesului la date şi a utilizării acestora de către consumatori şi întreprinderi”[6], precum şi „instituirea de garanţii împotriva transferului ilegal de date fără notificare din partea furnizorilor de servicii de *cloud”*[7].

Prezenta lucrare se va axa în principal pe a doua propunere de regulament, analizând principalele dispoziţii ale acesteia, în special, din perspectiva societăţilor care furnizează dispozitivele *smart*, urmând să fie tratate principalele soluţii legislative identificate de Comisia Europeană referitoare la problemele existente în practică privind dreptul de acces la date.

---

[2] Federal Trade Commission Staff Report, Internet of Things Privacy & Security in a Connected World, January 2015, p. 14, [Online] disponibil pe internet la adresa: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf, accesat la data de 07.06.2022.

[3] Propunere de Regulament al Parlamentului European și al Consiliului privind guvernanța datelor la nivel european (Legea privind guvernanța datelor), [Online] disponibil pe internet la adresa: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52020PC0767&from=EN, accesat la data de 07.06.2022.

[4] *Idem,* p. 1.

[5] Propunere de Regulament al Parlamentului European și al Consiliului privind normele armonizate pentru un acces echitabil la date și o utilizare corectă a acestora (Legea privind datele), [Online] disponibilă pe internet la adresa: https://op.europa.eu/en/publication-detail/-/publication/c83fe50f-9660-11ec-b4e4-01aa75ed71a1/language ro/format-PDF?msclkid=3ca7c617be6d11ecbf0bd71def53ebb1, accesat la data de 07.06.2022.

[6] *Idem,* p. 3.

[7] *Ibidem.*

1. Principalele provocări existente la momentul actual privind dreptul de acces la date

Potrivit documentului de lucru al serviciilor Comisiei Europene ce însoţeşte Legea privind datele, una dintre principalele provocări cu care se confruntă întreprinderile şi consumatorii constă în incapacitatea acestora de a beneficia de folosinţa datelor, întrucât le lipseşte controlul efectiv asupra acestora[8]. Cu această problemă se confruntă nu doar consumatorii, dar şi întreprinderile terţe, în special, cele din domeniul construcţiilor sau sectorul agricol.

Astfel, un exemplu în care o întreprindere nu are acces în mod efectiv la datele colectate de bunurile pe care le deţine în folosinţă sau chiar în proprietate, este ipoteza unui tractor al cărui sistem de frânare are incorporaţi senzori ce colectează datele necesare funcţionării acestuia. Fiind un dispozitiv ce aparţine IoT, în caz de defecţiune, poate fi reparat doar de furnizorul tractorului, întrucât cererile de acces la datele necesare formulate de întreprinderile terţe sunt respinse fără justificare, fapt ce duce şi la existenţa unor costuri mai mari datorită exclusivităţii serviciului[9]. În acest sens, potrivit asociaţiei *Zentralverband Deutsches Handwerk*[10] costurile serviciilor de reparaţii ar urma să scadă cu aproximativ 40% în cazul în care consumatorii sau întreprinderile ar putea să se adreseze unor terţe persoane.

În ceea ce priveşte consumatorii, în majoritatea cazurilor, aceştia nu pot apela la un terţ care le poate oferi avantaje suplimentare faţă de cele propuse de producători, cum ar fi costuri reduse sau setări care să permită o utilizare mai eficientă a energiei electrice de către dispozitivele *smart*, întrucât terţului îi este refuzat accesul la datele colectate de acestea. Prin urmare, putem afirma că în prezent producătorii de obiecte *smart* se bucură de o exclusivitate „de facto" asupra datelor în detrimentul utilizatorilor sau altor întreprinderi.

În acelaşi timp, apare problema naturii datelor generate de către aceste dispozitive, care pot fi atât cu caracter personal, cât şi fără caracter personal, respectiv a dispoziţiilor legale aplicabile în cazul acestora.

---

[8] Commision Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), [Online] disponibil pe internet la adresa:
https://op.europa.eu/en/publication-detail/-/publication/d0f2ed7a-9664-11ec-b4e4-01aa75ed71a1/language-en?msclkid=57a2cd84be7311ecbcec1ac33dd13ca9, accesat la data de 07.06.2022.

[9] *Idem*, p. 10.

[10] *Feedback* de la: Zentralverband des Deutschen Handwerk, [Online] disponibil pe internet la adresa:
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-amended-rules-on-the-legal-protection-of-databases/F2660174_en, accesat la data de 06.06.2022, accesat la data de 07.06.2022.

Astfel, pentru a asigura un grad de protecţie ridicat datelor cu caracter personal a fost elaborat Regulamentul (UE) 2016/679[11], ce defineşte la art. 4 pct. 1 noţiunea de date cu caracter personal ca fiind *orice informaţii privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.* Din interpretarea textului legal, rezultă în mod evident faptul că majoritatea persoanelor care achiziţionează un dispozitiv *smart* pot fi calificate drept persoane vizate, întrucât pe lângă datele fără caracter personal cum ar fi cele privind temperatura camerei, multe dispozitive *smart* colectează date privind locaţia în care se află.

Un alt text legal care interesează prezenta lucrare este cel de la art. 15 care reglementează dreptul de acces al persoanei vizate la datele gestionate de operatorul de date. Potrivit acestuia, persoana vizată, în cazul nostru cumpărătorul are dreptul să obţină de la operatorul de date acces la datele sale cu caracter personal. De asemenea, persoana vizată are dreptul să obţină acces la o serie de informaţii, cum ar fi *scopurile prelucrării, categoriile de date cu caracter personal vizate, destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din ţări terţe sau organizaţii internaţionale.* Aparent, legiuitorul European a asigurat suficiente pârghii legale pentru a securiza un grad ridicat de protecţie persoanelor vizate, instituind în sarcina operatorilor de date o serie de obligaţii suplimentare. Cu toate acestea, ipotezele în care persoanele vizate se adresează cu o cerere pentru a obţine acces la datele cu caracter personal colectate sunt extrem de rare.

În ceea ce priveşte datele fără caracter personal, sunt incidente dispoziţiile din Regulamentul 2018/1807[12], care urmăreşte să *asigure libera circulaţie a datelor, altele decât datele cu caracter personal, în cadrul Uniunii, prin stabilirea de norme privind cerinţele de localizare a datelor, disponibilitatea datelor pentru autorităţile competente şi portarea datelor pentru utilizatorii profesionişti.* Observăm preocuparea legiuitorului European în ceea ce priveşte portarea datelor fără caracter personal pentru utilizatorii profesionişti, dedicând în acest sens art. 6

[11] 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 95/46/CE (Regulamentul general privind protecția datelor), [Online] disponibil pe internet la adresa: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679&from=RO, accesat la data de 06.06.2022.

[12] Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană, [Online] disponibil pe internet la adresa: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32018R1807&from=RO, accesat la data de 06.06.2022.

potrivit căruia *Comisia încurajează şi facilitează elaborarea unor coduri de conduită de autoreglementare la nivelul Uniunii („coduri de conduită"), pentru a contribui la o economie competitivă a datelor*, în special prin asigurarea celor mai bune *practici pentru a facilita schimbarea furnizorilor de servicii şi portarea datelor într-un format structurat, utilizat în mod curent şi care poate fi prelucrat electronic.*

La o scurtă analiză a textelor legale rezultă că dispoziţiile privind portabilitatea datelor se aplică în cazul utilizatorilor profesionişti, adică o *persoană fizică sau juridică, inclusiv o autoritate publică sau un organism de drept public, care utilizează ori solicită un serviciu de prelucrare a datelor în scopuri legate de activitatea sa comercială, industrială, artizanală sau profesională ori de sarcinile sale.* Prin urmare, respectivele dispoziţii legale urmează să se aplice în cadrul relaţiei dintre producătorii de dispozitive *smart* şi întreprinderile care utilizează aceste dispozitive în activitatea lor profesională, neaplicându-se în cazul consumatorilor care au achiziţionat dispozitivele *smart* pentru a le utiliza într-un scop privat.

Luând în considerare faptul că, în majoritatea cazurilor, „datele cu caracter personal sunt combinate cu datele fără caracter personal"[13], am putea afirma că în cazul datelor colectate prin intermediul IoT predomină datele mixte. Se pune problema şi în acest caz care ar fi dispoziţiile legale incidente, cele din Regulamentul 2016/679 sau cele din Regulamentul 2018/1807? Răspunsul la această întrebare este oferit de art. 2 alin. 2 din Regulamentul 2018/1807 potrivit căruia *în cazul unui set de date compus atât din date cu caracter personal, cât şi din date fără caracter personal, prezentul regulament se aplică părţii din set cu date fără caracter personal. În cazul în care datele cu caracter personal şi cele fără caracter personal dintr-un set de date sunt legate între ele în mod indisolubil, prezentul regulament nu aduce atingere aplicării Regulamentului (UE) 2016/679.* Rezultă că se aplică fiecare Regulament în parte, respectiv Regulamentul 2018/1807 pentru datele fără caracter personal şi Regulamentul 2016/679 pentru datele cu caracter personal colectate de dispozitivele *smart.*

În acelaşi timp, potrivit tezei a doua din articolul anterior citat, reiese faptul că în cazul în care datele sunt indisolubil legate între ele urmează să aplice Regulamentul 2016/679. Cu toate acestea, nu există o definiţie legală a noţiunii de date indisolubile, în doctrină considerându-se că „datele sunt legate indisolubil atunci când un set de date conţine date din ambele categorii, iar separarea celor două tipuri de date, fie este imposibilă, fie este considerată de către operator ca ineficientă din punct de vedere economic sau nefezabilă din punct de vedere tehnic"[14].

[13] C.T. Ungureanu, *Drept internațional privat european în raporturi de comerț internațional*, Editura Hamangiu, București, 2021, p. 110.

[14] *Idem*, p. 111.

2. Noutăţi legislative. Soluţii propuse de către Comisia Europeană în ceea ce priveşte dreptul de acces la date

Pentru a răspunde la provocările existente pe piaţă, Comisia Europeană prin Legea privind datele, instituie o serie de obligaţii întreprinderilor al căror obiect de afaceri are legătură cu IoT.

În primul rând, este reglementat dreptul utilizatorilor de a accesa şi utiliza datele generate prin utilizarea produselor sau serviciilor conexe. Astfel, o parte dintre întreprinderile de pe piaţa IoT care nu informează clientul în mod explicit asupra drepturilor de acces la aceste date urmează să-şi modifice politica de activitate, fiind obligate în acest sens de art. 3 din Legea privind datele. Potrivit acestui articol, *înainte de încheierea unui contract de cumpărare, de închiriere sau de leasing al unui produs sau al unui serviciu conex, utilizatorului i se furnizează, într-un format clar şi inteligibil, natura şi volumul datelor care ar putea fi generate prin utilizarea produsului sau a serviciului conex, dacă este probabil ca datele să fie generate în mod continuu şi în timp real, precum şi modul în care utilizatorul poate accesa datele respective.* De asemenea, în cazul în care datele urmează să fie utilizate de o terţă persoană, furnizorul este obligat să informeze asupra acestui fapt utilizatorul, indicând *scopurile în care vor fi utilizate datele respective.*

Din dispoziţia anterior menţionată rezultă şi faptul că produsele *smart* urmează să fie proiectate *astfel încât datele generate prin utilizarea lor să fie, în mod implicit, accesibile utilizatorului cu uşurinţă, în mod securizat şi, când este relevant şi indicat, în mod direct.* Aceste obligaţii ar putea duce la modificarea unor lanţuri întregi de producţie a întreprinderilor care proiectau produsele în aşa mod încât accesul la date să fie restricţionat, precum şi la redactarea unor noi politici de confidenţialitate în care să se prevadă în mod explicit drepturile utilizatorului de acces asupra datelor colectate de produsele *smart.*

În al doilea rând, este prevăzut în mod expres faptul că deţinătorul de date, care, în majoritatea cazurilor, este chiar furnizorul de produse *smart,* poate să folosească *eventualele date fără caracter personal generate prin utilizarea unui produs sau a unui serviciu conex* numai în baza unui acord contractual cu utilizatorul. Rezultă că, în unele cazuri, consumatorii ar putea cere o remuneraţie în schimbul accesului la aceste date, în special, cei care folosesc IoT în afaceri.

De asemenea, utilizatorului i se recunoaşte dreptul de a partaja datele colectate de obiectele *smart* cu părţi terţe, chiar dacă această terţă persoană „oferă un serviciu post-vânzare potenţial concurent cu un serviciu furnizat de deţinătorul de date sau însărcinarea deţinătorului de date să facă acest lucru”[15]. Pentru a fi protejat deţinătorul de date, nici utilizatorul, nici partea terţă, nu pot utiliza datele pe care le primesc *pentru dezvoltarea unui produs care concurează cu produsul din care provin datele accesate sau pentru partajarea datelor cu altă parte terţă în scopul respectiv.*

Noile obligaţii presupun, în unele cazuri, reproiectarea obiectelor *smart,* aspect ce duce la suportarea unor cheltuieli suplimentare de către furnizorii de

[15] Legea privind datele, considerentul 28, p. 27.

produse sau servicii conexe. Dacă în cazul societăţilor mari, care au resurse suficiente, aceste obligaţii nu ar impune costuri extrem de oneroase, în cazul întreprinderilor mici şi mijlocii şi a „întreprinderilor din sectoarele tradiţionale ale căror capacităţi digitale sunt mai puţin dezvoltate aceste obligaţii ar avea un caracter excesiv de împovărător”[16]. Prin urmare, pentru a nu împiedica dezvoltarea sectorului IoT prin impunerea noilor restricţii, Legea privind datele exclude de la aplicarea respectivelor dispoziţii legale microîntreprinderile şi întreprinderile mici.

3. Obligaţia de a pune datele colectate la dispoziţia organismelor din sectorul public

O altă noutate legislativă reglementată de Legea privind datele constă în impunerea în sarcina deţinătorului de date, adică în majoritatea cazurilor furnizorul de produse IoT, a obligaţiei de a pune datele colectate de obiectele *smart la dispoziţia organismelor din sectorul public şi a instituţiilor, agenţiilor sau organelor Uniunii pe baza unei nevoi excepţionale*. În acest sens, potrivit art. 15 din propunerea de regulament se consideră că *există o nevoie excepţională de utilizare a datelor, în înţelesul prezentului capitol, atunci când datele solicitate sunt necesare pentru răspunsul la o urgenţă publică sau când cererea de date este limitată în timp şi ca domeniu de aplicare şi este necesară pentru prevenirea unei urgenţe publice sau pentru sprijinirea redresării în urma unei urgenţe publice*. Prin urmare, în cazul *urgenţelor rezultate din degradarea mediului şi dezastrele naturale majore, inclusiv cele agravate de schimbările climatice, precum şi dezastrele majore antropogene, cum ar fi incidentele majore de securitate cibernetică,* interesul public care rezultă din utilizarea datelor va prevala asupra intereselor deţinătorilor de date de a dispune liber de datele pe care le deţin.

Procedura presupune existenţa unei cereri din partea unui organism sau instituţii din sectorul public, care trebuie să precizeze ce date sunt solicitate şi să demonstreze existenţa nevoii excepţionale pentru care acestea se solicită. De asemenea, se va indica data-limită până la care respectivele date trebuie să fie puse la dispoziţia organismului sau instituţiei. Deţinătorul de date, care primeşte cererea, trebuie să ofere accesul la acestea fără întârzieri nejustificate, având totuşi dreptul de a refuza cererea sau să solicite modificarea acesteia în cazul în care datele nu sunt disponibile.

În acelaşi timp, deşi este prevăzut la art. 17 alin. 2 lit. d), faptul că o cerere formulată de organismul public *trebuie să se refere, în măsura posibilului, la date fără caracter personal*, ar putea exista situaţii când va fi oferit accesul şi la alt tip de date. Pentru a oferi un grad de protecţie celor de la care au fost colectate datele cu caracter personal, se instituie obligaţia în sarcina deţinătorului de date, adică furnizorul de produse IoT, de a *depune eforturi rezonabile pentru a pseudonimiza datele, în măsura în care cererea poate fi îndeplinită cu ajutorul unor date pseudonimizate*. Din cauză că aceste date sunt doar pseudonimizate, ci nu

[16] *Idem*, considerentul 36, p. 30.

anonimizate, urmează să se aplice dispoziţiile din Regulamentul 2016/679, întrucât aceste date continuă să fie considerate date cu caracter personal.

Pentru ca datele să nu rămână o perioadă îndelungată în posesia autorităţilor publice, la art. 19 au fost reglementate o serie de obligaţii în acest sens. Spre exemplu, autoritatea publică nu va putea utiliza *datele într-un mod incompatibil cu scopul pentru care au fost solicitate*, iar în cazul în care nu mai are nevoie de datele solicitate este obligată să le distrugă de îndată, urmând să informeze deţinătorul de date despre acest fapt.

Astfel, pe lângă necesitatea de a acorda acces la datele colectate de produsele *smart* consumatorilor, întreprinderile trebuie să fie pregătite să acorde într-un termen scurt acces la datele colectate de dispozitivele *smart* şi organismelor sau instituţiilor publice. În principiu, nu ar trebui să existe diferenţe semnificative între cele două proceduri, întrucât datele vor fi colectate şi stocate în acelaşi loc, iar etapele ce trebuie să fie parcurse pentru obţinerea accesului sunt aproape identice.

4. Soluţii noi la problemele vechi

Am menţionat anterior faptul că prin Regulamentul 2018/1807, furnizorii de servicii sunt încurajaţi „să redacteze şi să aplice efectiv coduri de conduită în scop de autoreglementare care să cuprindă bune practici pentru, printre altele, facilitarea trecerii la alţi furnizori de servicii de prelucrare a datelor şi portarea datelor”[17]. Potrivit constatărilor Comisiei, cadrele de autoreglementare elaborate în acest sens au o eficacitate limitată şi prin urmare este necesar să se adopte „un set de obligaţii minime de reglementare pentru furnizorii de servicii de prelucrare a datelor, în vederea eliminării barierelor contractuale, economice şi tehnice din calea trecerii efective de la un serviciu de prelucrare a datelor la altul”[18].

În acest sens, potrivit art. 23 şi următoarele din Legea privind datele, sunt prevăzute măsuri menite să asigure trecerea de la un furnizor de prelucrare a datelor la altul într-un termen optim şi cu costuri rezonabile. Astfel, o întreprindere care are drept obiect de activitate un domeniu în care se utilizează tehnologii IoT poate încheia un contract cu un furnizor de prelucrare a datelor având garanţia că în cazul în care doreşte să încheie un contract cu alt furnizor perioada de trecere la acesta ar dura maxim 30 de zile. Acest aspect rezultă din interpretarea textului legal reglementat de art. 24 alin. 1 lit. a) potrivit căruia părţile trebuie să stipuleze în contract clauze care să îi permită clientului, la cerere, *să treacă la un serviciu de prelucrare a datelor oferit de alt furnizor de servicii de prelucrare a datelor sau să porteze toate datele, aplicaţiile şi activele digitale generate direct sau indirect de client la un sistem de la faţa locului, în special să stabilească o perioadă de tranziţie maximă obligatorie de 30 de zile calendaristice.*

În ceea ce priveşte taxele de trecere la noul furnizor, se tinde la eliminarea acestora prin reglementarea în art. 25 a unei perioade de tranziţie. Astfel, pentru

[17] *Idem*, Considerentul nr. 70, p. 37.
[18] *Ibidem.*

început, furnizorii de servicii de prelucrare a datelor vor putea impune taxe de valoare redusă pentru procesul de trecere la alt furnizor, ca peste o perioadă, care urmează să fie stabilită odată cu intrarea în vigoare a Legii privind datele, acestea să fie eliminate.

Prin facilitarea accesului la alţi furnizori de servicii de prelucrare a datelor au de câştigat nu doar întreprinderile mici şi mijlocii care suportă clauze, de multe ori, abuzive, întrucât procesul de tranziţie la alt furnizor presupune existenţa unor costuri suplimentare pe care asemenea întreprinderi nu îşi pot permite să le onoreze, dar şi consumatorii care vor putea achiziţiona obiectele *smart* la un preţ mai mic. De asemenea, prin acest fapt se asigură şi o circulaţie a datelor de la un furnizor la altul mult mai sigură prin impunerea obligaţiei de cooperare între aceştia în perioada de tranziţie, aspect important pentru toate părţile implicate.

5. Transferul internaţional de date fără caracter personal

În final, o altă noutate legislativă, care are efect şi asupra sectorului IoT în ceea ce priveşte securitatea datelor fără caracter personal, constă în reglementarea în cadrul capitolului VII din Legea privind datele a unor garanţii suplimentare ce au drept obiect *prevenirea transferului internaţional de date fără caracter personal deţinute în Uniune sau accesul administraţiilor publice la astfel de date în cazul în care un astfel de transfer sau acces ar crea un conflict cu dreptul Uniunii sau cu dreptul intern al statului membru în cauză.*

În primul rând este prevăzut în mod expres faptul că *orice decizie sau hotărâre a unei instanţe judecătoreşti sau a unui tribunal şi orice decizie a unei autorităţi administrative a unei ţări terţe prin care se solicită unui furnizor de servicii de prelucrare a datelor să transfere date fără caracter personal intrând în domeniul de aplicare al prezentului regulament şi deţinute în Uniune sau să acorde acces la astfel de date poate fi recunoscută sau executabilă în orice mod doar dacă se bazează pe un acord internaţional, cum ar fi un tratat de asistenţă judiciară reciprocă, în vigoare între ţara terţă solicitantă şi Uniune sau pe orice alt asemenea acord între ţara terţă solicitantă şi un stat membru.*

Observăm o diferenţă faţă de dispoziţiile din Regulamentul 2016/679 potrivit cărora *orice date cu caracter personal care fac obiectul prelucrării sau care urmează a fi prelucrate după ce sunt transferate într-o ţară terţă sau către o organizaţie internaţională pot fi transferate doar dacă, sub rezerva celorlalte dispoziţii ale prezentului regulament, condiţiile prevăzute în prezentul capitol sunt respectate de operator şi de persoana împuternicită de operator, inclusiv în ceea ce priveşte transferurile ulterioare de date cu caracter personal din ţara terţă sau de la organizaţia internaţională către o altă ţară terţă sau către o altă organizaţie internațională.* Astfel, spre deosebire de situaţia datelor fără caracter personal care pot fi transferate către un stat terţ doar dacă se bazează pe un acord internaţional, în cazul datelor cu caracter personal, acest transfer este posibil în ipotezele în care Comisia a emis o decizie *privind nivelul adecvat al nivelului de protecţie* existent în statul terţ. De asemenea, se reglementează ipoteza în care o astfel de decizie

lipseşte, fiind stipulat în sarcina operatorului de date sau a persoanei împuternicită de acesta obligaţia de a oferi *garanţii adecvate* în acest sens.

Cu toate acestea, în cadrul art. 27 din Legea privind datele este prevăzut că datele fără caracter personal pot fi transferate către un stat terţ chiar dacă nu există un acord internaţional între Uniunea Europeană sau statul membru şi statul terţ, cu condiţia ca să fie respectate dispoziţiile prevăzute la alin. 3 din respectivul articol. Astfel, furnizorul va putea transfera datele obţinute din exploatarea unui dispozitiv *smart* către un stat terţ, dacă în acest stat *instanţa judecătorească competentă sau tribunalul competent care emite decizia sau hotărârea judecătorească ori care revizuieşte decizia unei autorităţi administrative are, în temeiul legislaţiei ţării respective, împuternicirea de a ţine seama în mod corespunzător de interesele juridice relevante ale furnizorului de date protejate de dreptul Uniunii sau de dreptul intern al statului membru în cauză.*

Pe lângă aceste garanţii, este prevăzută obligaţia în sarcina *furnizorului de servicii de prelucrare a datelor de a-l informa pe deţinătorul datelor cu privire la existenţa unei cereri din partea unei autorităţi administrative dintr-o ţară terţă de a i se acorda accesul la datele sale înainte de a da curs cererii, cu excepţia cazurilor în care cererea serveşte unor scopuri de asigurare a respectării legii şi atât timp cât acest lucru este necesar pentru a se menţine eficacitatea activităţii de asigurare a respectării legii.* Considerăm acest aspect important, întrucât prin recunoaşterea unui drept de acces asupra datelor în favoarea utilizatorului, se stabileşte implicit şi un drept de „proprietate" asupra respectivelor date. Astfel, utilizatorul de la care au fost colectate datele fără caracter personal ar fi interesat să fie informat asupra modului de utilizare a acestor date, având tot dreptul de a refuza transferul acestora către o autoritate dintr-un stat terţ, cu excepţia situaţiilor prevăzute de lege.

Concluzii

Aşadar, prin ultimele propuneri legislative la nivelul Uniunii începe să se creioneze un regim juridic în ceea ce priveşte dreptul de acces la date. Astfel, dacă anterior propunerii de Regulament, puteam discuta despre existenţa unui monopol asupra datelor colectate prin intermediul utilizării dispozitivelor *smart* de către furnizor, în viitor, în cazul în care Regulamentul va intra în vigoare fără modificări semnificative, acest monopol ar putea fi limitat prin recunoaşterea dreptului de acces al utilizatorului la aceste date. În acelaşi timp, dreptul furnizorului de obiecte sau servicii conexe de a avea acces la aceste date nu este limitat în aşa mod încât să existe consecinţe negative asupra dezvoltării sectorului IoT. Astfel, în relaţia cu consumatorii, întreprinderile vor trebui doar să prevadă în contractul pe care-l încheie dispoziţii suplimentare privind dreptul utilizatorului de acces la date. Apreciem că acest drept, în majoritatea cazurilor, nu va fi utilizat în mod efectiv. Prin urmare, dispoziţiile respective vor fi standardizate şi comunicate în acelaşi mod cum sunt prevăzute condiţiile de utilizare pe care puţini consumatori le citesc.

Totuşi, întreprinderile care folosesc obiectele *smart* în activitatea lor profesională ar putea cere o remuneraţie sau orice alt beneficiu în schimbul datelor fără caracter personal generate prin utilizarea acestor dispozitive, ca urmare a

prevederii din Legea privind datele care impune existenţa unui acord contractual pentru utilizarea acestor date de către deţinătorul de date. De asemenea, pentru a evita influenţa întreprinderilor mari în raport cu cele noi pe piaţă, care ar impune în mod unilateral clauze abuzive în legătură cu dreptul de acces la date de către utilizatori, în Legea privind datele a fost prevăzută o prezumţie de clauză abuzivă în art. 13 pct. 4 lit. c). Potrivit textului legal o clauză contractuală este prezumată clauză abuzivă dacă conţinutul acesteia are ca obiect *împiedicarea părţii căreia i-a fost impusă unilateral să utilizeze datele furnizate sau generate de partea respectivă pe durata contractului sau limitarea utilizării unor astfel de date în aşa măsură încât partea respectivă nu are dreptul să utilizeze, să înregistreze, să acceseze sau să controleze astfel de date sau să exploateze valoarea unor astfel de date în mod proporţional.*

Pe lângă acestea, se consideră că Legea privind datele va avea un impact în întreaga Uniune în ceea ce priveşte inovarea şi crearea unor noi locuri de muncă. Spre exemplu, furnizorii de servicii post-vânzare „vor putea să-şi îmbunătăţească serviciile şi să concureze pe picior de egalitate cu serviciile comparabile oferite de producătorii de dispozitive *smart*"[19]. Astfel, utilizatorii de produse IoT ar putea alege o persoană terţă care oferă servicii de reparaţii sau întreţinere mai ieftine. Această posibilitate le este recunoscută prin reglementarea unui drept de acces asupra datelor colectate de producătorul de obiecte *smart*, fapt ce va duce şi la reducerea costurilor acestor produse, în unele cazuri chiar ar putea prelungi durata de viaţă a acestora.

În concluzie, consider că în viitorul apropiat întreprinderile vor obţine un control efectiv asupra datelor fără caracter personal generate de obiectele *smart*, având dreptul de a cere o contraprestaţie în schimb. În ceea ce priveşte consumatorii, este nevoie de dezvoltarea continuă a educaţiei în domeniul digital pentru ca aceştia să înţeleagă importanţa şi posibilităţile oferite de datele colectate de dispozitivele *smart* pe care le procură.

Referinţe

Comisia Europeană, *Shaping Europe's digital future* [Online]

Commision Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) [Online]

Federal trade commission Staff Report, Internet of Things Privacy & Security in a Connected World, January 2015, p. 14 [Online]

Propunere de Regulament al Parlamentului European şi al Consiliului privind guvernanţa datelor la nivel european (Legea privind guvernanţa datelor) [Online]

Propunere de Regulament al Parlamentului European şi al Consiliului privind normele armonizate pentru un acces echitabil la date şi o utilizare corectă a acestora (Legea privind datele) [Online]

Ungureanu C.T., *Drept internaţional privat european în raporturi de comerţ internaţional*, Editura Hamangiu, Bucureşti, 2021

[19] Comisia Europeană, *Shaping Europe's digital future* [Online], disponibil pe internet la adresa: https://digital-strategy.ec.europa.eu/ro/node/10725, accesat la data de 07.06.2022