GRUPUL DE LUCRU „ARTICOLUL 29” PENTRU PROTECȚIA DATELOR

1471/14/RO
WP 223

Avizul 8/2014 privind evoluțiile recente din sfera internetului obiectelor

adoptat la 16 septembrie 2014

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL,

instituit prin Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995,

având în vedere articolele 29 și 30 din directiva respectivă,

având în vedere regulamentul său de procedură,

ADOPTĂ PREZENTUL AVIZ:

REZUMAT

Internetul obiectelor (IoT, *Internet of Things*) este pe cale de a deveni parte integrantă din viața cetățenilor europeni. Deși multe proiecte din domeniul internetului obiectelor nu și-au dovedit încă viabilitatea, în prezent dispunem de „obiecte inteligente” care ne monitorizează casele, mașinile, mediul de lucru și activitățile fizice și care comunică cu acestea. În ziua de azi există deja dispozitive conectate care reușesc să satisfacă nevoile cetățenilor UE pe marile piețe ale sinelui cuantificat și ale domoticii. Internetul obiectelor oferă astfel perspective semnificative de creștere pentru un mare număr de companii inovatoare și creatoare din UE, de mici și mari dimensiuni, care sunt prezente pe aceste piețe.

Grupul de lucru „articolul 29” dorește ca așteptările în acest domeniu să se realizeze, atât în interesul cetățenilor, cât și al întreprinderilor din UE. Beneficiile preconizate trebuie totuși să țină cont de numeroasele provocări pe care internetul obiectelor le poate reprezenta pentru viața privată și pentru securitate. Se nasc multe întrebări legate de vulnerabilitatea acestor dispozitive, care deseori sunt instalate în afara unei structuri IT clasice și nu încorporează într-o măsură suficientă caracteristici integrate de securitate. Pierderea datelor, infectarea cu programe malware, dar și accesul neautorizat la datele cu caracter personal, utilizarea intruzivă a electronicii vestimentare sau supravegherea ilegală constituie tot atâtea riscuri pe care părțile interesate din internetul obiectelor trebuie să le abordeze pentru a atrage potențiali utilizatori finali ai produselor sau serviciilor lor.

Dincolo de respectarea normelor juridice și tehnice, importante sunt de fapt implicațiile pe care internetul obiectelor le-ar putea avea asupra societății în general. Organizațiile care pun protecția vieții private și a datelor în centrul procesului lor de dezvoltare a produselor vor fi în măsură să se asigure că protecția vieții private este integrată în bunurile și serviciile lor încă din momentul conceperii și că aceste bunuri și servicii sunt configurate în mod implicit pentru a asigura respectarea vieții private, în concordanță cu așteptările cetățenilor UE.

Pentru moment, această analiză nu a fost menționată decât în termeni foarte generali de către mai multe autorități de reglementare și părți interesate din UE și din afara acesteia. Grupul de lucru „articolul 29” a decis să aprofundeze această temă prin adoptarea prezentului aviz, intenționând astfel să contribuie atât la aplicarea uniformă a cadrului juridic în materie de protecție a datelor în ceea ce privește internetul obiectelor, cât și la crearea unui nivel ridicat de protecție în ceea ce privește protecția datelor cu caracter personal în UE. Conformitatea cu acest cadru este esențială pentru a face față provocărilor descrise mai sus, care sunt de ordin juridic și tehnic, dar și societal, dat fiind faptul că protecția datelor este considerată un drept fundamental al omului.

Prin urmare, în prezentul aviz se identifică mai întâi principalele riscuri pe care protecția datelor le întâmpină în ecosistemul reprezentat de internetul obiectelor și apoi se oferă orientări cu privire la modul în care cadrul juridic al UE ar trebui să fie aplicat în acest context. Grupul de lucru sprijină ideea ca părțile interesate relevante să integreze în proiectele lor garanții de cel mai înalt nivel posibil pentru utilizatori. Mai precis, utilizatorii trebuie să dețină în permanență controlul deplin asupra datelor lor cu caracter personal de-a lungul întregului ciclu de viață al produsului și, atunci când organizațiile au nevoie de consimțământul lor pentru prelucrarea datelor respective, să își dea consimțământul în totală cunoștință de cauză, în deplină libertate și în mod specific pentru prelucrarea în cauză. Pentru a le ajuta pe diferitele părți interesate (fabricanți de dispozitive, dezvoltatori de aplicații, platforme sociale, alți destinatari ai datelor, platforme de date și organisme de standardizare) să îndeplinească obiectivul menționat mai sus, grupul de lucru a elaborat un set cuprinzător de

recomandări practice adresate acestora și menite să le ajute să integreze protecția vieții private și a datelor în produsele și serviciile lor.

Trebuie spus că pentru sprijinirea încrederii și a inovației, deci a reușitei pe aceste piețe, este esențial ca utilizatorii să fie responsabilizați prin informare permanentă, prin asigurarea libertății și prin garantarea siguranței lor. Grupul de lucru crede cu tărie că părțile interesate care îndeplinesc aceste așteptări vor avea un avantaj deosebit de mare față de concurenții ale căror modele de afaceri se bazează pe ascunderea, față de clienții lor, a măsurii în care datele acestora sunt prelucrate și comunicate altora și pe închiderea clienților în ecosistemele lor.

Grupul de lucru „articolul 29" va monitoriza evoluția internetului obiectelor, având în vedere provocările majore pe care acesta le reprezintă pentru protecția datelor. În acest scop, grupul continuă să fie deschis la cooperarea cu alte autorități de reglementare și alți legiuitori la nivel național și internațional în aceste chestiuni. De asemenea, grupul continuă să fie deschis la discuțiile cu reprezentanții societății civile, precum și cu cei ai sectoarelor în cauză, mai ales atunci când părțile interesate respective sunt operatori de date sau persoane împuternicite de aceștia în cadrul UE.

INTRODUCERE

Conceptul de internet al obiectelor (IoT) se referă la o infrastructură în care miliarde de senzori integrați în dispozitive obișnuite, folosite în viața de zi cu zi – „obiecte" ca atare sau obiecte legate de alte lucruri sau persoane – sunt proiectați astfel încât să înregistreze, să prelucreze, să stocheze și să transfere date și, pe baza unor identificatori unici care le-au fost atribuiți, să interacționeze cu alte dispozitive sau sisteme datorită capacităților de comunicație în rețea. Bazându-se pe principiul prelucrării ample de date prin intermediul acestor senzori proiectați să comunice în mod discret și să facă schimb de date în mod continuu, internetul obiectelor este strâns legat de noțiunile de informatică „omniprezentă" sau „ubicuă".

Părțile interesate din sfera internetului obiectelor își propun să ofere noi aplicații și servicii prin colectarea și combinarea ulterioară a acestor date referitoare la indivizi – fie pentru a măsura „exclusiv" datele specifice mediului utilizatorului, fie pentru a observa și a analiza în mod specific comportamentele acestuia. Cu alte cuvinte, internetul obiectelor presupune, de obicei, prelucrarea datelor care au legătură cu persoane fizice identificate sau identificabile și care întrunesc, așadar, criteriile necesare pentru a fi considerate date cu caracter personal în înțelesul articolului 2 din Directiva UE privind protecția datelor cu caracter personal.

Prelucrarea unor astfel de date în acest context se bazează pe intervenția coordonată a unui număr semnificativ de părți interesate (fabricanți de echipamente – care uneori funcționează și ca platforme de date, agregatori sau brokeri de date, dezvoltatori de aplicații, platforme sociale, organizații sau persoane care dau sau iau cu împrumut dispozitive etc.). Diferitele roluri ale acestor părți interesate vor fi analizate în continuare în prezentul aviz. Diversele părți interesate ar putea fi implicate din varii motive, respectiv pentru că se dorește furnizarea unor funcții suplimentare sau a unor interfețe de control ușor de folosit care permit gestionarea setărilor tehnice și a setărilor de confidențialitate sau pentru că, în general, utilizatorul are acces la datele colectate care îl privesc prin intermediul unei interfețe web distincte. În plus, datele stocate pe un server pot fi comunicate și altor părți, uneori fără ca persoana în cauză să aibă cunoștință de acest lucru[1]. În astfel de cazuri, utilizatorul este obligat să accepte ca datele sale să fie transmise mai departe și nu poate împiedica acest lucru fără să dezactiveze

[1] http://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf

majoritatea funcțiilor dispozitivului. Ca urmare a acestei înlănțuiri de activități, internetul obiectelor îi poate aduce pe fabricanții de dispozitive și pe partenerii lor comerciali în situația de a crea sau de a accesa profiluri de utilizator foarte detaliate.

Având în vedere cele de mai sus, este limpede că evoluția internetului obiectelor este însoțită de provocări noi și semnificative pentru protecția datelor cu caracter personal și pentru viața privată[2]. Într-adevăr, dacă nu sunt controlate, anumite evoluții ale internetului obiectelor ar putea merge până la o formă de supraveghere a indivizilor care ar putea fi considerată ilegală în temeiul dreptului UE. De asemenea, internetul obiectelor creează preocupări serioase în ceea ce privește securitatea, dat fiind că din încălcarea normelor de securitate pot rezulta riscuri semnificative pentru viața privată a indivizilor ale căror date sunt prelucrate în astfel de contexte.

Prin urmare, Grupul de lucru „articolul 29" a decis să emită prezentul aviz pentru a contribui la identificarea și monitorizarea riscurilor care decurg din aceste activități, atunci când sunt în joc drepturile fundamentale ale cetățenilor UE.

[2] Prezentul aviz ar trebui, de asemenea, să fie citit împreună cu avizele anterioare adoptate de grupul de lucru în 2014, și anume avizul referitor la aplicarea conceptelor de necesitate și proporționalitate și de protecția datelor în domeniul aplicării legii (WP 211) și avizul privind supravegherea (WP 215)

1. Domeniul de aplicare al avizului: accent special pe trei evoluții ale internetului obiectelor

În acest stadiu nu se poate prezice cu certitudine măsura în care se va dezvolta internetul obiectelor, în parte deoarece, în general, nu se poate încă spune în ce mod toate datele colectate eventual în internetul obiectelor se vor transforma în ceva util și deci viabil din punct de vedere comercial. Este, de asemenea, neclară eventuala convergență și raporturile de sinergie între internetul obiectelor și alte evoluții tehnologice, cum ar fi *cloud computing* și analitica predictivă, care, în prezent, privesc doar evoluțiile unor piețe emergente.

Prin urmare, Grupul de lucru „articolul 29" a decis ca în prezentul aviz să se concentreze, în mod special, asupra a trei evoluții specifice ale internetului obiectelor (informatica vestimentară, sau *wearable computing* în engleză, sinele cuantificat, sau *quantified self* și domotica) care 1) sunt în interfață directă cu utilizatorul și 2) corespund unor dispozitive și servicii utilizate în prezent, pretându-se astfel unei analize în temeiul dispozițiilor privind protecția datelor. Prin urmare, în prezentul aviz nu sunt tratate în mod specific nici aplicațiile B2B, nici temele mai generale, precum „orașele inteligente", „transporturile inteligente" sau evoluțiile din domeniul M2M („de la mașină la mașină"). Cu toate acestea, principiile și recomandările formulate în prezentul aviz pot fi aplicate în afara domeniului său strict de aplicare și pot fi valabile și pentru alte evoluții din domeniul internetului obiectelor, precum cele menționate mai sus.

1.1 **Informatica vestimentară**

Informatica vestimentară se referă la obiectele și articolele de îmbrăcăminte din viața de zi cu zi, cum ar fi ceasurile sau ochelarii, ale căror funcții au fost extinse prin montarea unor senzori. Obiectele informatice vestimentare au toate șansele să fie adoptate rapid, deoarece ele extind utilitatea obiectelor de uz cotidian care sunt familiare individului – cu atât mai mult cu cât nu pot fi diferențiate de sosiile lor neconectate. În dispozitivele de acest fel pot să fie încorporate camere, microfoane și senzori care pot să înregistreze date și să le transfere către fabricantul dispozitivului. În plus, disponibilitatea unei interfețe de programare a aplicației (API) pentru dispozitivele de informatice vestimentare (Android Wear[3], de exemplu) permite, de asemenea, crearea de aplicații de către terți, care pot avea astfel acces la datele colectate de aceste obiecte.

1.2 **Sinele cuantificat/cuantificarea sinelui**

Obiectele de cuantificare a sinelui sunt proiectate să fie purtate cu regularitate de către indivizii care doresc să înregistreze informații despre propriile obiceiuri și stiluri de viață. De exemplu, dacă cineva vrea să aibă o imagine detaliată asupra tiparelor sale de somn poate să poarte în fiecare noapte un dispozitiv de urmărire a somnului. Alte dispozitive, cum ar fi contoarele de activitate, sunt axate pe urmărirea mișcărilor. Dispozitivele de acest fel măsoară și afișează în continuu o serie de indicatori cantitativi legați de diferitele activități fizice ale unui individ, cum ar fi numărul de calorii arse sau distanțele parcurse pe jos.

Unele obiecte măsoară în plus greutatea, pulsul sau alți indicatori de sănătate. Prin observarea tendințelor și a schimbărilor survenite în comportament de-a lungul timpului, datele colectate pot fi analizate pentru a se deduce informații calitative despre starea sănătății, cum ar fi evaluări ale calității și efectelor activității fizice pe baza unor praguri prestabilite și, într-o anumită măsură, eventuala prezență a unor simptome de boală.

[3] http://developer.android.com/wear/index.html

Pentru a permite extragerea unor informații relevante, deseori este necesar ca senzorii de cuantificare a sinelui să fie purtați în anumite condiții. De exemplu, un accelerometru care este prins de cureaua unei persoane vizate și care conține algoritmii corespunzători poate să măsoare mișcările abdomenului *(date brute)*, să extragă informații despre ritmul respirației *(date agregate și informații extrase)* și să afișeze nivelul de stres al persoanei respective *(date afișabile)*. Unele dispozitive nu comunică utilizatorului decât acest ultim tip de date, însă fabricantul dispozitivului sau furnizorului serviciului poate avea acces la mult mai multe date care pot fi analizate ulterior.

Sinele cuantificat este problematic în ceea ce privește tipurile de date colectate care au legătură cu sănătatea, deci care sunt potențial sensibile, precum și în ceea ce privește colectarea extinsă a unor astfel de date. Întrucât se concentrează pe a-i motiva pe utilizatori să-și mențină o stare de sănătate bună, această mișcare are de fapt numeroase legături cu ecosistemul reprezentat de e-sănătate. Investigații recente au pus însă sub semnul întrebării exactitatea reală a măsurătorilor și a deducțiilor făcute pe baza acestora[4].

1.3 **Domotica**

În prezent, internetul obiectelor intră și în birourile sau locuințele noastre, unde pot fi instalate dispozitive „conectate" precum becuri, termostate, alarme detectoare de fum, stații meteorologice, mașini de spălat rufe sau cuptoare care pot fi controlate de la distanță prin intermediul internetului. De exemplu, există obiecte dotate cu senzori de mișcare care pot detecta și înregistra prezența utilizatorului în casă și eventualele regularități în deplasările acestuia și care pot declanșa eventual acțiuni specifice identificate în prealabil (cum ar fi aprinderea luminii sau reglarea temperaturii). Majoritatea dispozitivelor de automatizare a casei sunt conectate în permanență și pot transmite date fabricantului.

Este evident că domotica este însoțită de provocări specifice în ceea ce privește protecția datelor și a vieții private, dat fiind că prin analizarea tiparelor de utilizare într-un astfel de context se pot afla informații despre stilul de viață, obiceiurile sau alegerile persoanelor dintr-o casă sau pur și simplu dacă acestea sunt acasă sau nu.

Cele trei categorii de dispozitive enumerate mai sus sunt reprezentative pentru cele mai multe dintre principalele amenințări pe care internetul obiectelor în starea sa actuală le prezintă pentru viața privată. De remarcat însă că aceste categorii nu se exclud una pe alta. De exemplu, dispozitivele „vestimentare", cum ar fi ceasurile inteligente, ar putea fi utilizate pentru monitorizarea ritmului cardiac, deci pentru o analiză specifică sinelui cuantificat.

2. Provocările prezentate de internetul obiectelor pentru protecția vieții private și a datelor

Grupul de lucru „articolul 29" a decis să emită prezentul aviz specific pornind de la premisa că internetul obiectelor prezintă mai multe provocări pentru protecția vieții private și a datelor, dintre care unele sunt noi, iar altele mai tradiționale, dar amplificate de creșterea exponențială a volumului de date prelucrate pe care îl presupune evoluția sa. Importanța aplicării cadrului juridic al UE în materie de protecție a datelor și a recomandărilor practice de mai jos care corespund acestui cadru trebuie privite prin prisma acestor provocări.

[4] http://bits.blogs.nytimes.com/2014/04/27/for-fitness-bands-slick-marketing-but-suspect-results

2.1 **Lipsa controlului și asimetria informațională**

Ca urmare a necesității de a furniza servicii omniprezente în mod discret, este posibil ca utilizatorii înșiși să fie, în practică, monitorizați de părți terțe, ceea ce poate conduce la situații în care utilizatorii pierd orice control asupra difuzării datelor lor, în funcție de modul – transparent sau opac – în care se efectuează colectarea și prelucrarea acestor date.

La un nivel mai general, în urma interacțiunii dintre obiecte, dintre obiecte și dispozitivele indivizilor, dintre indivizi și alte obiecte, precum și dintre obiecte și sisteme centrale (*back-end*), vor fi generate fluxuri de date care nu pot fi gestionate cu instrumentele clasice utilizate pentru asigurarea nivelului adecvat de protecție a intereselor și drepturilor persoanelor vizate. De exemplu, spre deosebire de alte tipuri de conținut, este posibil ca datele generate de internetul obiectelor să nu poată fi revăzute în mod adecvat de persoana vizată înainte de publicarea lor, ceea ce, fără îndoială, generează un risc de lipsă de control din partea utilizatorului și de autoexpunere excesivă a acestuia. De asemenea, comunicarea dintre obiecte poate fi declanșată atât automat, cât și ca urmare a unei setări implicite, fără ca individul să fie conștient de acest lucru. Dacă nu există posibilitatea de a controla efectiv modul în care interacționează obiectele sau de a fixa limite virtuale prin stabilirea unor zone active sau inactive pentru anumite lucruri, controlarea fluxului de date generat va deveni o sarcină extrem de dificilă. O sarcină încă și mai dificilă va fi aceea de a controla utilizarea ulterioară a datelor respective și, astfel, de a preveni potențialele denaturări ale funcțiilor. Această problemă a lipsei de control, care privește și alte evoluții tehnologice, cum ar fi *cloud computing* și *big data*, este cu atât mai complexă dacă ne gândim că aceste diferite tehnologii emergente pot fi utilizate în combinație.

2.2 **Calitatea consimțământul utilizatorului**

În multe cazuri este posibil ca utilizatorul să nu aibă cunoștință de procesul de prelucrare a datelor efectuat de anumite obiecte. Această lipsă de informații constituie un obstacol semnificativ atunci când trebuie să se demonstreze consimțământul valabil în conformitate cu dreptul UE, întrucât persoana vizată trebuie să fie informată. În astfel de circumstanțe, consimțământul nu poate fi invocat ca bază juridică pentru prelucrarea datelor corespunzătoare în temeiul dreptului UE.

În plus, dispozitivele vestimentare, cum ar fi ceasurile inteligente, nu sunt ușor identificabile[5]. Majoritatea observatorilor nu pot face distincția între un ceas normal și un ceas conectat, chiar dacă în acesta din urmă pot fi integrate camere, microfoane și senzori de mișcare capabili să înregistreze și să transfere date fără știrea indivizilor și chiar fără ca aceștia să consimtă la o astfel de prelucrare. Se pune astfel problema identificării prelucrării de date prin intermediul informaticii vestimentare, problemă care ar putea fi rezolvată dacă s-ar avea în vedere o semnalizare corespunzătoare care ar fi efectiv vizibilă pentru persoanele vizate.

În plus, cel puțin în unele cazuri, posibilitatea de a renunța la anumite servicii sau elemente ale unui dispozitiv IoT este mai mult un concept teoretic decât o alternativă reală. Astfel de situații pun sub semnul întrebării libertatea – deci valabilitatea în temeiul dreptului UE – a consimțământului utilizatorului pentru prelucrarea de date subiacentă.

În plus, se poate ca mecanismele clasice utilizate pentru obținerea consimțământului indivizilor să fie greu de aplicat în cazul internetului obiectelor, ceea ce are ca rezultat un consimțământ de o „calitate slabă”, bazat pe lipsa informațiilor, sau imposibilitatea practică a unui consimțământ specific și

[5] Astfel cum se descrie în Avizul nr. 02/2013 privind aplicațiile instalate pe dispozitivele inteligente, informatica vestimentară scoate în evidență și provocări legate de colectarea continuă de date de la alte persoane din imediata apropiere și pentru perioade lungi de timp.

detaliat, care să reflecte preferințele exprimate de indivizi. În practică, se pare că, în prezent, dispozitivele cu senzori nu sunt, în general, proiectate nici pentru a furniza informații în mod autonom, nici pentru a oferi un mecanism valabil de obținere a consimțământului individului. Cu toate acestea, părțile interesate din domeniul internetului obiectelor ar trebuie să aibă în vedere noi moduri de obținere a consimțământului valabil al utilizatorului, cum ar fi prin introducerea unor mecanisme de obținere a consimțământului chiar în dispozitive. Mai jos în documentul de față sunt menționate exemple specifice, precum serverele proxy care permit protejarea vieții private (*privacy proxies*) și politicile lizibile automat care se lipesc de date (*sticky policies*).

2.3 **Deducțiile formulate pe baza datelor și utilizarea datelor prelucrate inițial în alte scopuri**

Creșterea volumului de date generate de internetul obiectelor, conjugată cu tehnicile moderne de analiză a datelor și de verificare încrucișată, poate determina utilizarea datelor respective în scopuri secundare care pot să aibă sau nu legătură cu scopul prelucrării inițiale. Este posibil astfel ca părțile terțe care solicită accesul la datele colectate de alte părți să dorească să utilizeze aceste date în scopuri complet diferite.

Date aparent nesemnificative care sunt colectate inițial prin intermediul unui dispozitiv (accelerometrul și giroscopul unui telefon inteligent, de exemplu) pot fi utilizate ulterior pentru deducerea altor informații cu o semnificație complet diferită (obiceiurile la volan ale individului, de exemplu). Această posibilitate de a formula deducții pe baza unor astfel de informații „brute” trebuie combinată cu riscurile clasice analizate în legătură cu fuziunea de date, un fenomen bine cunoscut în informatică[6].

Cuantificarea sinelui ilustrează, de asemenea, cantitatea de informații care poate fi dedusă din senzorii de mișcare prin agregare și analiză avansată. Aceste dispozitive utilizează deseori senzori elementari pentru captarea de date brute (mișcările persoanei vizate, de exemplu) și se bazează pe algoritmi complecși pentru extragerea unor informații practice (numărul de pași, de exemplu) și pentru deducerea unor informații potențial sensibile care vor fi afișate utilizatorilor finali (condiția fizică, de exemplu).

Această tendință este însoțită de provocări specifice. Mai exact, chiar dacă nu a avut nimic împotrivă să partajeze informațiile inițiale într-un anumit scop, utilizatorul ar putea să nu dorească să partajeze și aceste informații secundare, care ar putea fi utilizate în scopuri complet diferite. Este important, așadar, ca părțile interesate din domeniul internetului obiectelor să se asigure, la fiecare nivel (date brute, extrase sau afișate), că datele sunt utilizate în scopuri pe deplin compatibile cu scopul inițial al prelucrării și că respectivele scopuri sunt cunoscute de către utilizator.

2.4 **Practicile intruzive de punere în evidență a tiparelor comportamentale și de stabilire de profiluri**

Chiar dacă mai multe obiecte diferite vor colecta separat informații izolate, o cantitate suficientă de date colectate și analizate ulterior poate revela aspecte specifice ale obișnuințelor, comportamentelor și preferințelor individului. După cum s-a văzut mai sus, generarea de cunoștințe din date banale sau chiar anonime va fi facilitată de proliferarea senzorilor și va favoriza apariția unor capacități importante de creare de profiluri.

[6] Fuziunea de date constă în combinarea unor date provenite de la senzori cu date provenite din diverse surse în vederea obținerii unor informații mai bune și mai precise decât ar fi posibil dacă sursele respective ar fi utilizate izolat.

Dincolo de aceasta, analitica bazată pe informațiile captate într-un mediu de internet al obiectelor ar putea permite detectarea, la un grad încă și mai ridicat de detaliere și exhaustivitate, a obiceiurilor de viață și a tiparelor comportamentale ale unui individ.

Este într-adevăr probabil ca această tendință să aibă un impact asupra modului în care individul se comportă în realitate, în același mod în care s-a demonstrat că utilizarea intensivă a CCTV a influențat în mod corespunzător comportamentul cetățenilor în spațiile publice. În cazul internetului obiectelor, această supraveghere potențială ar putea pătrunde în sfera cea mai privată a vieții unui individ, inclusiv în casa sa, ceea ce va pune presiune pe individ, făcându-l să vrea să evite un comportament neobișnuit și să împiedice astfel detectarea a ceea ce ar putea fi perceput ca anomalie. O astfel de evoluție ar fi deosebit de intruzivă în viața privată și în intimitatea indivizilor și ar trebui monitorizată îndeaproape.

2.5 **Limitările posibilității de păstrare a anonimatului în contextul utilizării serviciilor**

Dezvoltarea deplină a capacităților internetului obiectelor ar putea să afecteze posibilitățile actuale de utilizare anonimă a serviciilor și, în general, să limiteze posibilitatea utilizatorilor de a rămâne neobservați.

De exemplu, dacă dispozitivele de informatică vestimentară sunt păstrate în imediata apropiere a persoanelor vizate, devin disponibili o serie de alți identificatori, cum ar fi adresele MAC (*Media Access Control*) ale altor dispozitive potențial utile pentru generarea unei amprente a dispozitivului (*fingerprint*) care ar permite geolocalizarea persoanei vizate. Colectarea adreselor MAC multiple și a dispozitivelor cu senzori multipli va contribui la crearea unor astfel de amprente unice și a unor identificatori mai stabili pe care părțile interesate din internetul obiectelor îi vor putea atribui unor indivizi specifici. Aceste amprente (*fingerprint*) și acești identificatori ar putea fi utilizați în mai multe scopuri, cum ar fi analitica pe baza poziției geografice[7] sau analiza tiparelor de deplasare a mulțimilor și a indivizilor.

Această tendință trebuie analizată împreună cu faptul că datele de acest fel pot fi ulterior combinate cu alte date publicate de alte sisteme (CCTV sau istorice de utilizare a internetului, de exemplu).

În astfel de situații, unele date provenite de la senzori sunt deosebit de vulnerabile la atacurile prin reidentificare.

Având în vedere cele de mai sus, este clar că va fi tot mai dificil pentru utilizatori să își păstreze anonimatul și să își protejeze viața privată în internetul obiectelor. Din acest punct de vedere, dezvoltarea internetului obiectelor este însoțită de preocupări semnificative legate de protecția datelor și a vieții private.

2.6 **Riscuri pentru securitate: securitate sau eficiență**

Internetul obiectelor prezintă o serie de provocări în materie de securitate. Fabricanții de dispozitive sunt obligați, pe baza cerințelor legate de securitate și resurse, să găsească un echilibru între eficiența bateriei și securitatea dispozitivului. Mai exact, încă nu este clar în ce mod fabricanții de dispozitive vor concilia introducerea măsurilor de confidențialitate, integritate și disponibilitate la toate nivelurile prelucrării de date cu necesitatea de a optimiza consumul de resurse de calcul – și de energie – de către senzori și obiecte.

[7] Analitica pe baza poziției geografice (*location analytics*) se referă la analizarea numărului de persoane care se află într-un anumit loc la un anumit moment și a intervalului de timp în care persoanele respective rămân în locul respectiv.

Există deci riscul ca internetul obiectelor să transforme obiecte de zi cu zi în potențiale ținte ale atacurilor la viața privată și la securitatea informațiilor și, în același timp, să extindă aceste ținte dincolo de versiunea actuală a internetului. Dispozitivele conectate mai puțin sigure ar putea deschide noi posibilități eficiente de atac, cum ar fi prin relaxarea practicilor de supraveghere sau încălcarea securității datelor, ceea ce poate avea ca rezultat furtul sau compromiterea datelor, acțiuni cu efecte considerabile asupra drepturilor consumatorilor și asupra modului în care indivizii percep securitatea internetului obiectelor.

Dispozitivele și platformele IoT ar urma, de asemenea, să facă schimb de date și să le stocheze în infrastructurile prestatorilor de servicii. Prin urmare, în cazul securității internetului obiectelor trebuie să se țină seama nu doar de securitatea dispozitivelor, ci și de legăturile de comunicații, de infrastructura de stocare și de alte elemente care fac parte din acest ecosistem.

Tot astfel, prezența unor niveluri diferite de prelucrare, care sunt proiectate și implementate de diferite părți interesate, nu asigură coordonarea adecvată între toate aceste părți interesate și ar putea avea ca rezultat existența unor puncte slabe care pot fi utilizate pentru exploatarea punctelor vulnerabile.

De exemplu, cea mai mare parte a senzorilor existenți în prezent pe piață nu au capacitatea de a stabili o legătură criptată de comunicare, întrucât capacitățile de calcul necesare pentru aceasta ar afecta dispozitivele care sunt limitate de o baterie slabă. În ceea ce privește securitatea de la un capăt la altul, rezultatul integrării unor componente fizice și logice furnizate de mai multe părți interesate garantează doar nivelul de securitate oferit de cea mai slabă componentă.

3. Aplicabilitatea dreptului UE în cazul prelucrării de date cu caracter personal în internetul obiectelor

3.1 **Dreptul aplicabil**

În UE, cadrul juridic relevant pentru evaluarea problemelor pe care internetul obiectelor le prezintă pentru protecția vieții private și a datelor în UE este reprezentat d3 Directiva 95/46/CE și de anumite dispoziții ale Directivei 2002/58/CE, astfel cum a fost modificată prin Directiva 2009/136/CE.

Acest cadru se aplică atunci când sunt îndeplinite condițiile pentru aplicarea sa prevăzute la articolul 4 din Directiva 95/46/CE. În Avizul nr. 8/2010 privind dreptul aplicabil[8], grupul de lucru a furnizat orientări detaliate cu privire la interpretarea dispozițiilor articolului 4.

Concret, în conformitate cu articolul 4 alineatul (1) litera (a) din directivă, dreptul intern al unui stat membru este aplicabil tuturor proceselor de prelucrare a datelor cu caracter personal desfășurate în contextul stabilirii operatorului pe teritoriul statului membru în cauză. Această noțiune de stabilire în contextul economiei bazate pe internet a fost recent interpretată într-un mod foarte larg de Curtea de Justiție a Uniunii Europene[9].

Dreptul intern al unui stat membru este aplicabil și în cazurile în care operatorul nu este stabilit pe teritoriul Comunității, dar utilizează „echipamente” situate pe teritoriul statului membru respectiv [articolul 4 alineatul (1) litera (c)]. Prin urmare, chiar dacă nu este stabilită pe teritoriul UE în înțelesul articolului 4 alineatul (1) litera (a), o parte interesată din domeniul internetului obiectelor (implicată în dezvoltarea, distribuția sau operarea dispozitivelor IoT) care întrunește criteriile pentru a fi considerată

[8] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_ro.pdf
[9] Hotărârea Curții (Marea Cameră) din 13 mai 2014, C-131/12, punctele 45-60.

operator de date în temeiul Directivei 95/46/CE se va supune probabil dreptului UE atunci când prelucrează date colectate prin intermediul „echipamentelor” unor utilizatori situați în UE.

De fapt, toate obiectele care sunt utilizate pentru a colecta și a prelucra ulterior datele unor indivizi în contextul prestării de servicii în internetul obiectelor întrunesc criteriile pentru a fi considerate echipamente în înțelesul directivei. Această încadrare se aplică, în mod evident, dispozitivelor propriu-zise (contoare de pași, dispozitive de urmărire a somnului, aparate menajere „conectate”, cum ar fi termostatele, alarmele de fum, ochelarii sau ceasurile conectate etc.). Ea se aplică, de asemenea, dispozitivelor terminale ale utilizatorilor (telefoane inteligente sau tablete, de exemplu) pe care în prealabil au fost instalate programe software sau aplicații atât pentru monitorizarea mediului utilizatorului cu ajutorul senzorilor integrați sau al interfețelor de rețea, cât și pentru trimiterea ulterioară a datelor colectate de aceste dispozitive către diferiții operatori de date implicați.

Pentru clarificarea statutului juridic – de operatori de date – al diferitele părți interesate din domeniul internetului obiectelor și, astfel, pentru determinarea dreptului național aplicabil prelucrării de date întreprinse de acestea, precum și a obligațiilor care le revin, va fi esențial să se stabilească rolul pe care îl au aceste părți. Modul în care se stabilește rolul părților interesate din domeniul internetului obiectelor va fi analizat în secțiunea 3.3 de mai jos.

3.2 **Noțiunea de date cu caracter personal**

Dreptul UE se aplică prelucrării datelor cu caracter personal, astfel cum sunt definite la articolul 2 din Directiva 95/46/CE. În Avizul nr. 4/2007 privind conceptul de date cu caracter personal[10], grupul de lucru a furnizat orientări detaliate cu privire la interpretarea acestei noțiuni.

În contextul internetului obiectelor se întâmplă adesea ca un individ să fie identificat pe baza unor date care provin de la „obiecte". Datele de acest fel pot permite recunoașterea modelului de viață al unui anumit individ sau al unei anumite familii – date generate de sistemul de comandă centralizată a iluminatului, încălzirii, ventilației și aerului condiționat, de exemplu.

În plus, ar putea fi nevoie ca și datele referitoare la indivizi care urmează să fie prelucrate numai după aplicarea unor tehnici de pseudonimizare sau chiar anonimizare să fie considerate date cu caracter personal. În realitate, cantitatea mare de date prelucrate automat în contextul internetului obiectelor presupune riscuri de reidentificare. În această privință, grupul de lucru recomandă consultarea recentului său aviz privind tehnicile de anonimizare în care sunt descrise evoluțiile relevante, care ajută la identificarea acestor riscuri și în care sunt formulate recomandări cu privire la aplicarea acestor tehnici[11].

3.3 **Părțile interesate din domeniul internetului obiectelor ca operatori cu sediul în UE**

Conceptul de operator și interacțiunea acestui concept cu cel de persoană împuternicită de către operator sunt esențiale în aplicarea Directivei 95/46/CE, dat fiind că ele condiționează responsabilitățile diverselor organizații implicate în efectuarea unei prelucrări de date în ceea ce privește normele UE în materie de protecție a datelor. Părțile interesate pot consulta Avizul 1/2010 al Grupului de lucru „articolul 29" privind conceptele de „operator" și „persoană împuternicită de către operator"[12], care oferă orientări cu privire la aplicarea acestui concept în cazul sistemelor complexe cu mai mulți actori, în care numeroase scenarii implică operatori și persoane împuternicite de aceștia care acționează singuri sau împreună cu alții și care prezintă diferite grade de autonomie și răspundere.

Concretizarea internetului obiectelor presupune ocazional intervenția combinată a mai multor părți interesate, precum fabricanții de echipamente, platformele sociale, aplicațiile de la terți, organizațiile sau persoanele care dau sau iau cu împrumut dispozitive, brokerii de date[13] sau platformele de date.

Dată fiind complexitatea rețelei de părți interesate, este necesar/obligatoriu să existe o repartizare precisă a responsabilităților între respectivele părți în ceea ce privește prelucrarea datelor personale ale indivizilor, pe baza particularităților intervențiilor lor respective.

3.3.1 Fabricanții de dispozitive

Fabricanții de dispozitive din domeniul internetului obiectelor nu fac doar să vândă articole fizice clienților lor sau produse *white label* altor organizații. În plus, ei pot să dezvolte sau să modifice sistemul de operare al „obiectului" sau să instaleze programe care determină funcționalitatea generală a acestuia, cum ar fi datele și frecvența de colectare, precum și momentul, destinatarul și scopul

[10] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_ro.pdf

[11] Avizul 05/2014 privind tehnicile de anonimizare adoptat la 10 aprilie 2014 (WP 216), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_ro.pdf

[12] Avizul 1/2010 privind conceptele de „operator" și „persoană împuternicită de către operator", adoptat la 16 februarie 2010 (WP 169) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_ro.pdf

[13] Brokerii de date cumpără date de la întreprinderi în vederea întocmirii unei liste de indivizi care aparțin aceleiași categorii sau aceluiași grup. Aceste categorii și grupuri sunt stabilite de către brokerii de date, dar pot reflecta caracteristici demografice, venituri sau interesul exprimat pentru o anumită temă sau un anumit produs.

transmiterii de date (de exemplu, societățile pot să calculeze valoarea asigurării angajaților lor pe baza datelor transmise de dispozitivelor de urmărire pe care le-au cerut angajaților să le poarte[14]). Majoritatea acestor fabricanți colectează și prelucrează, de fapt, datele cu caracter personal care sunt generate de dispozitiv în scopuri pe care le-au stabilit integral, întrunind astfel criteriile pentru a fi considerați operatori de date în temeiul dreptului UE.

3.3.2 Platformele sociale

Probabilitatea ca persoanele vizate să utilizeze obiecte conectate este chiar mai mare atunci când persoanele respective pot face publice datele sau când le pot partaja cu alți utilizatori. În special utilizatorii de dispozitive de cuantificare a sinelui au tendința să partajeze date cu alte persoane în rețelele de socializare, pentru a promova o formă de concurență pozitivă în cadrul grupului.

Acest tip de partajare în rețelele de socializare a datelor colectate și agregate de „obiecte" are loc deseori în mod automat, imediat după ce utilizatorul și-a configurat aplicația în acest sens. Această funcție de partajare face parte din configurația standard a aplicațiilor oferite de fabricant.

Agregarea acestor rapoarte pe platformele sociale înseamnă că acestora din urmă li se aplică din momentul respectiv anumite responsabilități în materie de protecție a datelor. Întrucât aceste date sunt încărcate de utilizator pe platformele sociale, atunci când acestea din urmă prelucrează datele în scopuri specifice, pe care le-au stabilit ele însele, întrunesc criteriile pentru a fi considerate operatori în nume propriu în temeiul dreptului UE, . De exemplu, o rețea de socializare poate utiliza informații colectate de un podometru pentru a deduce că un anumit utilizator aleargă cu regularitate și pentru a-i prezenta acestuia reclame la încălțăminte de alergat. Consecințele acestei încadrări au fost prezentate în detaliu în avizul Grupului de lucru „articolul 29" referitor la rețelele de socializare[15].

3.3.3 Dezvoltatorii terți de aplicații

Mulți senzori expun API-urile pentru a facilita dezvoltarea de aplicații. Pentru a utiliza aceste aplicații, persoanele vizate trebuie să instaleze aplicații ale unor terți prin care aceștia din urmă obțin acces la datele persoanelor respective, astfel cum sunt stocate de fabricantul dispozitivului. Instalarea acestor aplicații presupune deseori că dezvoltatorul de aplicații primește acces la date prin intermediul API.

Anumite aplicații îi pot recompensa pe utilizatorii anumitor obiecte. De exemplu, o aplicație dezvoltată de o societate de asigurări de sănătate i-ar putea recompensa pe utilizatorii de „obiecte" de cuantificare a sinelui sau o societate de asigurări imobiliare ar putea dezvolta o aplicație specială pentru a se asigura că alarmele de incendiu conectate ale clienților săi sunt configurate corect. Dacă aceste date nu sunt anonimizate în mod corespunzător, un astfel de acces constituie o prelucrare în temeiul articolului 2 din Directiva 95/46/CE, ceea ce înseamnă că dezvoltatorul de aplicații care a organizat acest acces la date trebuie considerat operator în temeiul dreptului UE.

Aplicațiile de acest gen sunt instalate obicei facultativ (*opt-in*). Întrucât un astfel de acces se supune cerinței de obținere a consimțământului prealabil al utilizatorului, acest consimțământ trebuie să fie acordat în clar, special pentru scopul indicat și în cunoștință de cauză. În practică însă, se întâmplă adesea ca cererile de autorizare depuse de către dezvoltatorii terți de aplicații să nu afișeze suficiente informații pentru a se considera că utilizatorul și-a dat consimțământul special pentru scopul indicat și

[14] Cu ajutorul dispozitivelor de urmărire, angajatorii pot urmări sănătatea lucrătorilor, http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

[15] Avizul 5/2009 privind socializarea în rețea online, adoptat la 12 iunie 2009 (WP 163), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_ro.pdf

în suficientă cunoștință de cauză și deci că acest consimțământ este valabil în temeiul dreptului UE (a se vedea mai jos).

3.3.4 Alți terți

Dispozitivele IoT pot fi utilizate și de alți terți, în afara fabricanților de dispozitive și a dezvoltatorilor terți de aplicații, pentru colectarea și prelucrarea de informații despre indivizi. De exemplu, societățile de asigurări de sănătate ar putea dori să ofere clienților lor podometre, pentru a monitoriza frecvența cu care aceștia fac mișcare[16] și pentru a le adapta în consecință primele de asigurare.

Spre deosebire de fabricanții de dispozitive, acești terți nu au niciun control asupra tipului de date colectate de obiect. Cu toate acestea, ei întrunesc criteriile pentru a fi considerați operatori pentru aceste prelucrări, în măsura în care colectează și stochează datele generate de astfel de dispozitive IoT în scopuri specifice pe care le-au stabilit ei înșiși.

Exemplu: o societate de asigurări lansează un nou program și oferă un contor de pași asiguraților care doresc să plătească prime mai scăzute. Asigurații care acceptă oferta primesc un contor de pași configurat și înregistrat de societate. Chiar dacă asigurații au acces la datele înregistrate de contoarele lor de pași, dispozitivele în sine sunt deținute de „FeelGood", care, la rândul său, are acces la datele asiguraților. În acest context, ar trebui ca asigurații să fie considerați persoane vizate și ca acestora să li se acorde acces la contul lor din aplicația de numărare a pașilor, dat fiind că societatea de asigurări întrunește criteriile pentru a fi considerată operator.

3.3.5 Platformele de date IoT

Din cauza unei lipse de standardizare și de interoperabilitate, internetul obiectelor este considerat uneori un „intranet al obiectelor", în care fiecare fabricant și-a definit propriul set de interfețe și propriul format de date. Datele sunt apoi găzduite în medii închise, care îi împiedică pe utilizatori să își transfere (sau chiar să își combine) datele de pe un dispozitiv pe altul.

Cu toate acestea, telefoanele inteligente și tabletele au devenit portalurile naturale prin care datele colectate prin intermediul numeroaselor dispozitive IoT ajung pe internet. Drept urmare, fabricanții au dezvoltat treptat platforme care își propun să găzduiască datele colectate prin intermediul acestor diferite dispozitive, în vederea centralizării și a simplificării gestionării lor.

Astfel de platforme pot, de asemenea, să fie considerate operatori în temeiul legislației UE în materie de protecție a datelor, atunci când dezvoltarea unor astfel de servicii implică de fapt colectarea în scopuri proprii a datelor cu caracter personal ale utilizatorilor.

[16] Cu ajutorul dispozitivelor de urmărire, angajatorii pot urmări sănătatea lucrătorilor, http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

3.4 **Indivizii ca persoane vizate: abonați, utilizatori și neutilizatori**

Abonații la internetul obiectelor și, în general, utilizatorii internetului obiectelor întrunesc criteriile pentru a fi considerați persoane vizate în temeiul dreptului UE. Dacă datele pe care le colectează și le stochează sunt utilizate exclusiv în scop personal sau casnic, utilizatorii intră sub incidența așa-numitei „excepții a activităților domestice" din Directiva 95/46/CE[17]. În practică însă, modelul de afaceri al internetului obiectelor presupune faptul că datele utilizatorului sunt sistematic transferate către fabricanții de dispozitive, dezvoltatorii de aplicații și alți terți care întrunesc criteriile pentru a fi considerați operatori. „Excepția activităților domestice" va avea, prin urmare, o aplicare limitată în contextul internetului obiectelor.

Prelucrarea datelor în internetul obiectelor poate viza și indivizii care nu sunt nici abonați, nici utilizatori efectivi ai internetului obiectelor. De exemplu, dispozitivele de informatică vestimentară, cum ar fi ochelarii, pot colecta date despre alte persoane vizate decât proprietarul dispozitivului. Este important să se sublinieze faptul că acest factor nu împiedică dreptul Uniunii să se aplice în astfel de situații. Aplicarea normelor UE în materie de protecție a datelor nu depinde de cine este proprietarul unui dispozitiv sau al unui terminal, ci de prelucrarea datelor cu caracter personal, indiferent de cine este individul vizat de aceste date.

4. Obligațiile care revin părților interesate din domeniul internetului obiectelor

Părțile interesate din domeniul internetului obiectelor care întrunesc criteriile pentru a fi considerate operatori (indiferent dacă acționează singure sau împreună cu alții) în temeiul dreptului UE trebuie să îndeplinească diferitele obligații care le revin în sensul Directivei 95/46/CE și al dispozițiilor relevante din Directiva 2002/58/CE, dacă este cazul. În prezentul aviz nu este abordată decât aplicarea dispozițiilor care necesită o atenție deosebită în acest context, dar această atenție limitată nu împiedică aplicarea celorlalte dispoziții.

4.1 **Aplicarea articolului 5 alineatul (3) din Directiva asupra confidențialității și comunicațiilor electronice**

Articolul 5 alineatul (3) din Directiva 2002/58/CE se aplică în situațiile în care o parte interesată din domeniul internetului obiectelor stochează informații sau dobândește acces la informațiile deja stocate pe dispozitive IoT, în măsura în care dispozitivele respective întrunesc criteriile pentru a fi considerate „echipamente terminale" în înțelesul dispoziției menționate[18]. Conform acestei dispoziții, abonatul sau utilizatorul în cauză trebuie să consimtă la stocare sau acces pentru ca aceste acțiuni să fie considerate legitime, mai puțin atunci când ele sunt strict necesare pentru furnizarea unui serviciu cerut în mod expres de către abonat sau utilizator[19]. Această cerință este cu atât mai importantă cu cât și alte părți interesate, în afară de utilizatori sau abonați, pot avea acces la informații confidențiale stocate în astfel de echipamente terminale[20].

Cerința de obținere a consimțământului, prevăzută la articolul 5 alineatul (3), se referă în primul rând la fabricantul dispozitivului, dar și la toate părțile interesate care doresc să aibă acces la aceste date

[17] A se vedea Avizul 5/2009 privind socializarea în rețea online, adoptat la 12 iunie 2009 (WP 163).
[18] Noțiunea de „echipament terminal" de la articolul 5 alineatul (3) trebuie înțeleasă în același mod ca cea de „echipamente" de la articolul 4 alineatul (1) litera (c).
[19] Avizul nr. 02/2013 privind aplicațiile instalate pe dispozitivele inteligente (WP 202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_ro.pdf
[20] A se vedea considerentul 25 din Directiva 2002/58/CE.

brute agregate care sunt stocate în infrastructura respectivă. Cerința se aplică, de asemenea, operatorilor de date care doresc să stocheze date suplimentare pe dispozitivul unui utilizator.

În astfel de circumstanțe, părțile interesate din domeniul internetului obiectelor trebuie să se asigure că persoana în cauză a consimțit efectiv la stocare și/sau acces, după ce a primit de la operator informații clare și cuprinzătoare cu privire la scopurile prelucrării, printre altele.

Prin urmare, consimțământul utilizatorului trebuie să fie obținut înainte de a accesa informații stocate pe dispozitiv care pot fi utilizate pentru a genera o amprentă (*fingerprint*) a dispozitivului (inclusiv dispozitive de informatică vestimentară). Grupul de lucru a emis deja orientări cu privire la noțiunea de consimțământ pentru modulele cookie sau tehnologiile similare de urmărire în documentul său de lucru 02/2013 (WP 208) și va furniza orientări suplimentare pe această temă în viitorul său aviz privind amprentarea dispozitivelor (*fingerprinting*).

Exemplu: un podometru înregistrează numărul de pași făcuți de utilizator și stochează aceste informații în memoria sa internă. Utilizatorul și-a instalat pe calculator o aplicație prin care descarcă direct din podometru informația referitoare la numărul de pași. Dacă dorește să încarce datele din podometre pe serverele sale, fabricantul dispozitivului trebuie să obțină consimțământul utilizatorului, astfel cum se prevede la articolul 5 alineatul (3) din Directiva 2002/58/CE.

După ce fabricantul dispozitivului a încărcat datele pe serverele sale, se păstrează numai date agregate cu privire la numărul de pași pe minut. Aplicațiile care cer acces la datele stocate pe serverul fabricantului dispozitivului nu se mai supun articolului 5 alineatul (3) din Directiva asupra confidențialității și comunicațiilor electronice, ci dispozițiilor referitoare la legitimitatea acestei prelucrări ulterioare din Directiva 95/46/CE.

În plus, proprietarul unui dispozitiv IoT și persoana ale cărei date vor fi monitorizate (persoana vizată) pot să nu fie una și aceeași persoană, ceea ce poate duce la o aplicare diferențiată a dispozițiilor, și anume fie a articolului 5 alineatul (3) din Directiva 2002/58/CE, fie a Directivei 95/46/CE.

Exemplu: un serviciu de închirieri auto instalează în automobilele sale un dispozitiv inteligent de urmărire a autovehiculelor. Deși se consideră că proprietarul/abonatul dispozitivului/serviciului de urmărire este serviciul de închirieri auto, individul care închiriază automobilul întrunește criteriile pentru a fi considerat utilizatorul dispozitivului. Conform articolului 5 alineatul (3), fabricantul dispozitivului trebuie (cel puțin) să obțină consimțământul utilizatorului dispozitivului, în acest caz al individului care închiriază automobilul. În plus, legitimitatea prelucrării datelor cu caracter personal referitoare la indivizii care închiriază automobile va intra sub incidența cerințelor distincte ale articolului 7 din Directiva 95/46/CE.

4.2 **Temeiul juridic pentru prelucrarea datelor (articolul 7 din Directiva 95/46/CE)**

Părțile interesate din domeniul internetului obiectelor care întrunesc criteriile pentru a fi considerate operatori (a se vedea secțiunea 4.3 de mai sus) trebuie să îndeplinească una dintre cerințele enumerate la articolul 7 din directiva menționată, pentru ca prelucrarea datelor cu caracter personal să fie legitimă. Aceste cerințe se aplică în cazul unora dintre aceste părți în plus față de aplicarea articolului 5 alineatul (3), atunci când prelucrarea în cauză presupune mai mult decât stocarea de informații sau dobândirea accesului la informații stocate în echipamentele terminale ale utilizatorului/abonatului[21].

[21] Pentru formularea articolului 5 alineatul (3) și a articolului 7 litera (a), a se vedea, în special, Avizul nr. 02/2013 privind aplicațiile instalate pe dispozitivele inteligente, adoptat la 27 februarie 2013 (WP 202), p. 14

În practică, în acest context sunt relevante trei temeiuri juridice.

Consimțământul [articolul 7 litera (a)] este primul temei juridic care ar trebui avut în vedere în contextul internetului obiectelor, atât de către fabricanții de dispozitive, cât și de platformele de socializare sau de date, de către organizațiile sau persoanele care dau cu împrumut dispozitive sau de către dezvoltatorii terți. În câteva rânduri, Grupul de lucru a emis, de asemenea, orientări cu privire la aplicarea simultană a cerințelor de la articolul 7 litera (a) și de la articolul 5 alineatul (3) din Directiva 2002/58/CE[22]. Condițiile pentru ca un astfel de consimțământ să fie valabil în temeiul dreptului UE au fost menționate și într-un aviz anterior al Grupului de lucru[23].

La articolul 7 litera (b) se prevede, de asemenea, că prelucrarea este legitimă dacă este necesară pentru executarea unui contract la care persoana vizată este parte. Domeniul de aplicare al acestui temei juridic este limitat de criteriul „necesității", conform căruia între prelucrarea propriu-zisă și scopurile executării contractului din partea persoanei vizate trebuie să existe o legătură directă și obiectivă.

În al treilea rând, în temeiul articolului 7 litera (f) se permite prelucrarea datelor cu caracter personal atunci când prelucrarea este necesară pentru realizarea interesului legitim urmărit de operator sau de către unul sau mai mulți terți cărora le sunt comunicate datele, cu condiția ca acest interes să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate – în special dreptul la respectarea vieții private în ceea ce privește prelucrarea datelor cu caracter personal – care necesită protecție în temeiul articolului 1 alineatul (1) din directivă.

În hotărârea pronunțată în cauza Google/Spania[24], Curtea de Justiție a Uniunii Europene a furnizat orientări importante cu privire la interpretarea acestei dispoziții, în plus față de cele furnizate în cauzele conexate anterioare ASNEF și FECEMD (C-468/10 și C-469/10). În contextul internetului obiectelor, există probabilitatea ca prelucrarea datelor cu caracter personal ale unui individ să afecteze în mod semnificativ drepturile fundamentale la respectarea vieții private și la protecția datelor cu caracter personal în situațiile în care, fără dispozitivele IoT, interconectarea datelor fie nu ar fi fost posibilă, fie ar fi fost posibilă doar cu mare dificultate. Astfel de situații pot apărea atunci când datele colectate se referă la starea de sănătate, casa, spațiul intim, poziția geografică și numeroase alte aspecte ale vieții private a unui individ. Este clar că o astfel de prelucrare – având în vedere posibila sa gravitate – nu poate fi justificată prin simplul interes economic pe care o parte interesată din domeniul internetului obiectelor îl are în prelucrarea respectivă. Trebuie să existe și alte interese urmărite de operator sau de terțul ori de terții cărora le sunt comunicate datele[25].

și urm., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_ro.pdf, și Avizul 06/2014 privind noțiunea de interese legitime ale operatorului de date prevăzută la articolul 7 din Directiva 95/46/CE (WP 217), p. 26, 32, 46

[22] Avizul WP 202, p. 14 și urm.

[23] Avizul nr. 15/2011 privind definiția consimțământului, adoptat la 13 iulie 2011, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_ro.pdf

[24] Hotărârea Curții (Marea Cameră) din 13 mai 2014, C-131/12, punctele 74 și urm.

[25] Avizul WP 217

Exemplu: în cadrul unui plan de promovare a utilizării transporturilor publice și de reducere a poluării, primăria dorește să reglementeze parcarea în centrul orașului prin impunerea unor restricții de acces, precum și a unor taxe de parcare. Valoarea taxei depinde de o serie de parametri, precum tipul de motor (motorină, benzină, electric) și vechimea autovehiculului. În momentul în care autovehiculul se apropie de un loc de parcare, plăcuța de înmatriculare a acestuia este citită de un senzor, în vederea calculării, după verificarea unei baze de date, a suprataxei sau a reducerii care se va aplica automat, conform unor criterii stabilite în prealabil. În acest caz, prelucrarea informațiilor conținute în plăcuța de înmatriculare pentru determinarea taxei ar putea fi în interesul legitim al operatorului. O eventuală prelucrare ulterioară, cum ar fi obținerea de informații – care nu au fost anonimizate – cu privire la circulația autovehiculelor în interiorul zonei restricționate ar necesita un alt temei juridic.

4.3 **Principiile referitoare la calitatea datelor**

Luate împreună, principiile consacrate la articolul 6 din Directiva 95/46/CE constituie o piatră de temelie a legislației UE în materie de protecție a datelor.

Datele cu caracter personal ar trebui colectate și prelucrate în mod corect și legal. Principiul corectitudinii presupune în mod special ca datele cu caracter personal să nu fie niciodată colectate și prelucrate fără ca individul să aibă cunoștință de acest lucru. Această cerință este cu atât mai importantă în ceea ce privește internetul obiectelor, cu cât senzorii sunt astfel proiectați încât să fie discreți, adică pe cât se poate invizibili. Cu toate acestea, operatorii care acționează în domeniul internetului obiectelor (în primul rând fabricanții de dispozitive) trebuie să îi informeze pe toți indivizii din vecinătatea geografică sau digitală a dispozitivelor conectate atunci când se colectează date referitoare la ei sau la mediul lor. Respectarea acestei dispoziții depășește cadrul unei cerințe strict legale, întrucât colectarea corectă face parte din cele mai importante așteptări ale utilizatorului în raport cu internetul obiectelor și în special cu informatica vestimentară.

Exemplu: un dispozitiv de sănătate utilizează un mic senzor luminos pentru monitorizarea modului în care circulă sângele prin vene și pentru obținerea de informații cu privire la bătăile inimii. Dispozitivul mai este prevăzut cu un senzor care măsoară nivelul de oxigen din sânge, însă datele colectate în acest sens nu sunt afișate nici pe dispozitiv, nici pe interfața utilizatorului. Chiar dacă senzorul de nivel de oxigen din sânge este pe deplin funcțional, acesta nu ar trebui activat fără încunoștințarea prealabilă a utilizatorului. Pentru activarea acestui senzor este necesar consimțământul explicit al utilizatorului.

Principiul limitării scopului presupune că datele pot fi colectate numai în scopuri precizate clar, explicite și legitime. O prelucrare ulterioară care este incompatibilă cu aceste scopuri inițiale ar fi ilegală în temeiul dreptului UE. Principiul ar trebui să permită utilizatorilor să știe cum și în ce scopuri le vor fi folosite datele și să decidă dacă își încredințează sau nu datele unui operator. Aceste scopuri trebuie definite *înainte* de prelucrarea efectivă a datelor, excluzându-se astfel posibilitatea unor modificări bruște în condițiile esențiale de prelucrare. Acest lucru presupune ca părțile interesate din domeniul internetului obiectelor să aibă o vedere clară de ansamblu asupra modelului lor de afaceri înainte de a începe să colecteze date cu caracter personal.

De asemenea, datele colectate cu privire la persoana vizată ar trebui să fie strict necesare pentru scopul specific stabilit în prealabil de către operator (principiul reducerii la minimum a datelor). Datele care nu sunt necesare pentru scopul respectiv nu ar trebuie să fie colectate „pentru orice eventualitate” sau pentru că „ar putea fi utile mai târziu”. Unele părți interesate consideră că principiul reducerii la minimum a datelor poate limita posibilitățile oferite de internetul obiectelor și poate constitui astfel o

barieră în calea inovării, pornindu-se de la ideea că din prelucrarea de date efectuată sub forma unei analize exploratorii, în vederea găsirii unor corelații și tendințe care nu sunt evidente, ar putea rezulta posibile avantaje. Grupul de lucru nu poate fi de acord cu o astfel de analiză și insistă asupra faptului că principiul reducerii la minimum a datelor joacă un rol esențial în apărarea drepturilor la protecția datelor pe care dreptul UE le prevede pentru indivizi, astfel încât el ar trebui respectat ca atare[26]. Acest principiu presupune în special că, atunci când datele cu caracter personal nu sunt necesare pentru furnizarea unui anumit serviciu bazat pe internetul obiectelor, persoanei vizate ar trebui cel puțin să i se ofere posibilitatea de a utiliza serviciul în mod anonim.

La articolul 6 se mai prevede că datele cu caracter personal colectate și prelucrate în contextul internetului obiectelor sunt păstrate o perioadă nu mai lungă decât este necesar în vederea atingerii scopului pentru care datele au fost colectate sau prelucrate ulterior. Acest test de necesitate trebuie să fie efectuat de fiecare dintre părțile implicate în furnizarea unui anumit serviciu prin internetul obiectelor, dat fiind că, în realitate, scopurile prelucrărilor lor pot fi diferite. De exemplu, datele cu caracter personal comunicate de către un utilizator în momentul în care se abonează la un anumit serviciu prin internetul obiectelor ar trebuie șterse imediat după ce utilizatorul se dezabonează. De asemenea, nu ar trebuie să se păstreze informațiile șterse de utilizator din contul său. Atunci când utilizatorul nu folosește serviciul sau aplicația pentru o perioadă definită de timp, profilul utilizatorului ar trebui inactivat. După o altă perioadă de timp, datele ar trebui șterse. Utilizatorul ar trebui să fie notificat înainte de efectuarea acestor acțiuni, prin orice mijloc de care dispune partea interesată relevantă.

4.4 **Prelucrarea datelor sensibile (articolul 8)**

Aplicațiile din internetul obiectelor pot prelucra date cu caracter personal din care se pot afla informații despre originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice, apartenența sindicală, starea sănătății sau viața sexuală, adică informații care întrunesc criteriile pentru a fi considerate „date sensibile” și care necesită, astfel, o protecție specială în înțelesul articolului 8 din Directiva 95/46/CE. În practică, aplicarea articolului 8 în cazul datelor sensibile din internetul obiectelor înseamnă că operatorii trebuie să obțină consimțământul explicit al utilizatorului, cu excepția cazului în care persoana vizată a făcut ea însăși publice datele respective.

O astfel de situație poate apărea în contexte specifice, cum ar fi dispozitivele de cuantificare a sinelui. În aceste cazuri, dispozitivele înregistrează preponderent date referitoare la starea de bine a individului. Aceste date nu constituie neapărat date medicale propriu-zise, însă pot furniza rapid informații despre sănătatea individului, întrucât sunt înregistrate în timp, permițând astfel desprinderea unor concluzii din variațiile intervenite într-un anumit interval de timp. Operatorii ar trebui să anticipeze această posibilă trecere într-o altă categorie și să ia măsurile adecvate în consecință.

[26] În orice caz, în practică cercetările exploratorii nu sunt niciodată efectuate complet la întâmplare . Scopul general al oricărei cercetări este, cel puțin parțial, în mod tradițional definit , fie numai și din motive organizatorice și bugetare. Este greu de imaginat că prelucrarea datelor pentru o cercetare specifică va fi compatibilă cu scopul inițial al colectării datelor, ceea ce va reprezenta o încălcare a legislației UE.

Exemplu: societatea X a dezvoltat o aplicație care, prin analizarea datelor brute de la semnalele de electrocardiogramă generate de senzori disponibili pe scară largă în comerț, are capacitatea de detecta tipare de dependență de droguri. Motorul aplicației poate extrage din datele brute de la EKG anumite caracteristici care, conform rezultatelor unor investigații anterioare, sunt legate de consumul de droguri. Produsul, care este compatibil cu majoritatea senzorilor de pe piață, ar putea fi utilizat ca aplicație de sine stătătoare sau prin intermediul unei interfețe web care presupune încărcarea datelor. Pentru prelucrarea datelor în acest scop ar trebui să se obțină consimțământul explicit al utilizatorului. Această cerință de obținere a consimțământului poate fi îndeplinită în aceleași condiții și în același timp cu obținerea consimțământului persoanei vizate în temeiul articolului 7 litera (a).

4.5 **Cerințele de transparență (articolele 10 și 11)**

Depășind cadrul cerinței de colectare corectă a datelor, astfel cum se prevede la articolul 6 litera (a), operatorii trebuie să comunice persoanelor vizate, în aplicarea articolelor 10 și 11, anumite informații: identitatea operatorului, scopul prelucrării, destinatarii datelor, existența dreptului la acces și a dreptului de opoziție (inclusiv informații despre modul în care obiectul poate fi deconectat, pentru a se evita divulgarea unor date suplimentare).

În funcție de aplicație, aceste informații ar putea să fi disponibile, de exemplu, chiar pe obiect, cu ajutorul conexiunii fără fir pentru difuzarea de informații sau cu ajutorul localizării prin testul de proximitate efectuat cu respectarea vieții private de un server centralizat pentru informarea utilizatorilor care se află în apropierea senzorului.

Aceste informații trebuie, în plus, să fie furnizate într-un mod clar și ușor de înțeles, conform principiului prelucrării corecte. De exemplu, fabricantul dispozitivului ar putea imprima pe obiectele dotate cu senzori un cod QR sau un *flashcode* care să descrie tipul de senzori și informațiile pe care acestea le captează, precum și scopurile în care sunt colectate datele respective.

4.6 **Securitatea (articolul 17)**

La articolul 17 din Directiva privind protecția datelor se prevede că operatorul trebuie să aplice „*măsuri tehnice și organizatorice de protecție adecvate pentru protejarea datelor cu caracter personal*” și „*dacă prelucrarea este efectuată pe seama sa, să aleagă o persoană [împuternicită] care să prezinte suficiente garanții referitoare la măsurile de securitate tehnică și de organizare privind prelucrarea care urmează să fie efectuată*”.

În consecință, orice parte interesată care întrunește criteriile pentru a fi considerată operator rămâne responsabilă pe deplin pentru securitatea prelucrării datelor. Dacă defectele de securitate care au ca rezultat încălcarea principiului securității sunt cauzate de un mod inadecvat de proiectare sau întreținere a dispozitivelor utilizate, este angajată răspunderea operatorului. În acest sens, este necesar ca acești operatori să evalueze securitatea sistemelor în ansamblu, inclusiv la nivel de componente, aplicând principiile securității părților componente. De asemenea, pentru dispozitivele respective trebuie să se recurgă la procedura de certificare și să se efectueze alinieri la standardele de securitate recunoscute la nivel internațional, în vederea îmbunătățirii securității generale a ecosistemului reprezentat de internetul obiectelor.

Subcontractanții care proiectează și fabrică componente de hardware în numele altor părți interesate, fără a prelucra efectiv date cu caracter personal, nu pot, strict vorbind, să fie considerați responsabili în temeiul articolului 17 din Directiva 95/46/CE în cazul în care protecția datelor este încălcată ca urmare a unui carențe de securitate la nivelul dispozitivelor respective. Aceste părți interesate au totuși un rol

esențial în menținerea securității ecosistemului reprezentat de internetul obiectelor. Părțile interesate care au responsabilități directe în materie de protecție a datelor față de persoanele vizate ar trebui să se asigure că acești subcontractanți respectă efectiv înalte standarde de securitate în ceea ce privește viața privată atunci când își proiectează și fabrică produsele.

După cum s-a afirmat anterior, la aplicarea măsurilor de securitate trebuie să se țină seama de limitele operaționale specifice ale dispozitivelor IoT. De exemplu, cei mai mulți senzori nu au în prezent capacitatea de a stabili o legătură criptată deoarece accentul se pune fie pe autonomia fizică a dispozitivului, fie pe controlul costurilor.

În plus, dispozitivele care funcționează în internetul obiectelor sunt, de asemenea, dificil de securizat, din motive atât tehnice, cât și comerciale. Întrucât componentele utilizează de obicei o infrastructură de comunicații fără fir și sunt caracterizate de resurse limitate în ceea ce privește energia și puterea de calcul, dispozitivele sunt vulnerabile la atacuri fizice, interceptări sau atacuri prin impregnarea sistemului (atacuri *proxy*). Tehnologiile utilizate cel mai des în prezent – și anume PKI (*Public Key Infrastructure*, infrastructură cu cheie publică) – nu sunt ușor suportate de dispozitivele IoT, deoarece majoritatea dispozitivelor nu dispun de puterea de calcul necesară pentru îndeplinirea sarcinilor de prelucrare cerute. Internetul obiectelor implică un lanț de aprovizionare complex, cu mai multe părți interesate care poartă grade diferite de răspundere. O eventuală încălcare a securității își poate avea originea la nivelul oricăreia dintre ele, mai ales în cazul mediilor M2M, care se bazează pe schimbul de date între dispozitive. Prin urmare, ar trebui să se țină seama de necesitatea de a utiliza protocoale sigure și suple, care se pretează la medii cu resurse reduse.

În acest context, Grupul de lucru „articolul 29” subliniază faptul că, atunci când capacitatea scăzută de calcul pune în pericol securitatea și eficiența comunicării, este și mai important să se respecte principiul reducerii la minimum a datelor și să se limiteze la minimul necesar prelucrarea de date cu caracter personal, în special stocarea acestora pe dispozitiv.

În plus, dispozitivele care sunt proiectate să fie accesate direct prin internet nu sunt întotdeauna configurate de utilizator. Există astfel riscul ca ele să ofere o cale ușoară de acces intrușilor, dacă sunt utilizate cu setările implicite. Practicile de securitate care se bazează pe restricții de rețea, pe dezactivarea implicită a funcțiilor neimportante și pe împiedicarea utilizării unor surse nefiabile de actualizare a programului software (și astfel pe limitarea atacurilor cu programe malware bazate pe modificarea codului) ar putea contribui la limitarea impactului și amplorii eventualelor cazuri de încălcare a securității. Aceste măsuri de securitate pentru protecția vieții private ar trebui să fie incorporate încă de la început, în aplicarea principiului de „luare în considerare a vieții private începând cu momentul conceperii”.

În plus, lipsa actualizărilor automate duce la vulnerabilități care deseori nu sunt rezolvate și care ar putea fi descoperite cu ușurință cu ajutorul unor motoare de căutare specializate. Chiar și în cazurile în care utilizatorii au cunoștință de vulnerabilitățile propriilor dispozitive, este posibil ca aceștia să nu aibă acces la actualizările vânzătorului, fie din cauza limitărilor hardware-ului , fie din cauză că tehnologiile sunt depășite și nu permit instalarea actualizărilor pe dispozitiv. În cazul în care un fabricant de dispozitive întrerupe serviciul de asistență pentru un dispozitiv, ar trebui oferite soluții alternative de asistență (cum ar fi deschiderea programului software pentru comunitatea programelor cu sursă deschisă). Utilizatorii trebuie să fie avertizați că dispozitivele lor ar putea deveni vulnerabile la defecte nereparate.

Unele dintre sistemele de autourmărire (cum ar fi podometrele sau dispozitivele de urmărire a somnului) care se găsesc pe piață prezintă, de asemenea, defecte de securitate care permit atacatorilor să falsifice valorile observate care sunt transmise aplicațiilor și fabricanților de dispozitive. Este esențial ca aceste dispozitive să ofere măsuri adecvate de protecție împotriva falsificării datelor, în special dacă valorile transmise de aceşti senzori au un impact indirect asupra deciziilor luate de utilizatori cu privire la sănătatea lor.

Nu în ultimul rând, existența unei proceduri adecvate de avertizare în cazul unei încălcări a securității datelor poate contribui, de asemenea, la controlarea efectelor negative ale vulnerabilităților de software și de proiectare prin asigurarea unei mai bune informării și prin furnizarea de îndrumări cu privire la aceste probleme.

5. Drepturile persoanelor vizate

Părțile interesate din domeniul internetului obiectelor trebuie să respecte drepturile persoanelor vizate, în conformitate cu dispozițiile prevăzute la articolele 12 și 14 din Directiva 95/46/CE, și să ia măsuri organizatorice în consecință. Aceste drepturi nu se limitează la abonații serviciilor de internet al obiectelor și la proprietarii de dispozitive. Ele îi privesc pe toți indivizii ale căror date cu caracter personal fac obiectul prelucrării.

5.1 **Dreptul de acces**

La articolul 12 litera (a) se prevede că persoanele vizate au dreptul să obțină de la operatori comunicarea într-o formă inteligibilă a datelor care fac obiectul prelucrării și a altor informații disponibile cu privire la originea datelor.

În practică, utilizatorii internetului obiectelor tind deseori să fie închiși în anumite sisteme. De obicei, dispozitivele trimit datele mai întâi la fabricant, care apoi oferă utilizatorului acces la datele respective prin intermediul unui portal internet sau al unei aplicații. Acest mod de proiectare permite fabricanților să pună la dispoziție servicii online care potențează capacitățile dispozitivelor, dar care, în același timp, i-ar putea împiedica pe utilizatori să aleagă în mod liber serviciul care să interacționeze cu dispozitivul lor.

În plus, rareori se întâmplă în prezent ca utilizatorii finali să aibă acces la datele brute care sunt înregistrate de dispozitivele IoT. Este evident că utilizatorii au un interes mai mare să aibă acces la datele interpretate decât la datele brute, pe care s-ar putea să nu le înțeleagă. Totuși, accesul la aceste date se poate dovedi util pentru ca utilizatorii finali să înțeleagă ce poate deduce despre ei fabricantul dispozitivului pe baza datelor respective. Dacă ar avea acces la aceste date brute, utilizatorii ar avea și posibilitatea de a-și transfera datele la alt operator și de a opta pentru alte servicii – de exemplu, în cazul în care operatorul inițial își schimbă politica de protecție a vieții private într-un mod care îi nemulțumește pe utilizatori. În prezent, utilizatorii nu au în practică nicio altă posibilitate decât să renunțe la utilizarea dispozitivelor lor, dat fiind că majoritatea operatorilor nu oferă o astfel de posibilitate și nu permit accesul decât la o versiune degradată a datelor brute stocate.

Grupul de lucru „articolul 29” consideră că astfel de atitudini împiedică exercitarea efectivă a dreptului de acces acordat indivizilor prin articolul 12 litera (a) din Directiva 95/46/CE. Acesta consideră, de asemenea, că părțile interesate din domeniul internetului obiectelor ar trebui să ia măsuri pentru a permite utilizatorilor exercitarea efectivă a acestui drept și să ofere utilizatorilor posibilitatea de a alege un alt serviciu, chiar dacă este vorba de un serviciu care este posibil să nu fie propus de fabricantul dispozitivului. În acest scop, ar fi util să se elaboreze standarde de interoperabilitate a datelor.

Întreprinderea unor astfel de măsuri ar fi cu atât mai relevantă, cu cât așa-numitul „drept la portabilitatea datelor” – care va fi probabil consacrat în Regulamentul general privind protecția datelor ca o variație a dreptului de acces – urmărește să pună capăt în mod clar situațiilor de „închidere în sistem” a utilizatorilor[27]. Țelul legiuitorului european în această chestiune este acela de a îndepărta obstacolele din calea concurenței și de a-i ajuta pe noii actori să inoveze pe această piață.

5.2 **Posibilitatea de revocare a consimțământului și de opoziție**

Persoanele vizate trebuie să aibă posibilitatea de a-și revoca eventualul consimțământ dat în prealabil pentru o anumită prelucrare de date și de a se opune prelucrării datelor care le privesc. Exercitarea acestor drepturi trebuie să fie posibilă fără constrângeri sau obstacole tehnice sau organizatorice, iar instrumentele puse la dispoziție pentru înregistrarea revocării ar trebui să fie accesibile, vizibile și eficiente.

Sistemele de revocare ar trebui să prezinte un grad ridicat de detaliere și să se refere la: (1) orice tip de date colectate de un anumit obiect (de exemplu, cererea ca stația meteorologică să întrerupă colectarea datelor despre umiditate, temperatură și sunete); (2) un anumit tip de date colectate de orice obiect (de exemplu, utilizatorul ar trebui să aibă posibilitatea de a întrerupe colectarea de date efectuată de orice dispozitiv care înregistrează sunete, fie că este vorba de un dispozitiv de urmărire a somnului ori de o stație meteorologică); (3) un anumit tip de prelucrare (de exemplu, utilizatorul ar putea să ceară ca atât podometrul, cât și cronometrul său să înceteze funcția de numărare a pașilor).

Întrucât este probabil ca „obiectele conectate” din informatica vestimentară să înlocuiască articole existente care oferă funcții obișnuite, operatorii ar trebui să ofere opțiunea de dezactivare a funcției „conectat” a obiectului (de exemplu în cazul ceasurilor sau al ochelarilor inteligenți), pentru ca acesta să poată funcționa la fel ca articolul original, cel neconectat. Grupul de lucru a precizat deja că persoanele vizate ar trebui să aibă posibilitatea de a-și revoca în orice moment consimțământul, fără a fi nevoiți să părăsească serviciul prestat[28].

Exemplu: un utilizator își instalează în apartament o alarmă de incendiu conectată. Alarma utilizează un senzor de prezență în casă, un senzor de căldură, un senzor de ultrasunete și un senzor de lumină. Dintre acești senzori, unii sunt necesari pentru detectarea unui incendiu, în timp ce alții oferă doar funcții suplimentare despre care utilizatorul a fost informat în prealabil. Utilizatorul ar trebui să aibă posibilitatea de a dezactiva funcțiile respective și de a utiliza numai alarma de incendiu, deci de a deconecta senzorii utilizați pentru celelalte funcții.

Este interesant de observat că unele evoluții recente în acest domeniu indică o încercare de capacitare a persoanelor vizate, prin faptul că li se acordă mai mult control asupra funcțiilor de gestionare a

[27] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_ro.pdf

[28] Avizul nr. 13/2011 privind serviciile de localizare geografică pe dispozitivele mobile inteligente, adoptat la 16 mai 2011 (WP 185), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_ro.pdf

consimțământului, de exemplu prin folosirea așa-numitelor politici *sticky*[29] sau a serverelor proxy care permit protejarea vieții private[30].

6. Concluzii și recomandări

Mai jos sunt prezentate o serie de recomandări pe care Grupul de lucru „articolul 29" a considerat că este util să le formuleze pentru a facilita aplicarea cerințelor juridice ale UE în cazul internetului obiectelor.

Recomandările de mai jos reprezintă doar orientări care vin în completarea documentelor care au fost adoptate anterior de Grupul de lucru „articolul 29".

În acest sens, Grupul de lucru dorește să atragă în mod special atenția asupra recomandărilor sale anterioare cu privire la aplicațiile instalate pe dispozitivele inteligente[31]. Întrucât telefoanele inteligente fac parte din mediul internetului obiectelor și ambele ecosisteme implică un set comparabil de părți interesate, aceste recomandări sunt direct relevante pentru internetul obiectelor. Mai precis, dezvoltatorii de aplicații și fabricanții de dispozitive ar trebui să le asigure utilizatorilor finali un nivel adecvat de informații și să ofere opțiuni de refuz și/sau de consimțământ pe categorii, dacă este cazul. În plus, atunci când consimțământul nu a fost obținut, operatorul ar trebui să anonimizeze datele înainte de a le utiliza în alte scopuri sau de a le comunica altor părți.

6.1 Recomandări pentru toate părțile interesate

- Înainte de lansarea oricărei noi aplicații în internetul obiectelor ar trebui efectuate evaluări ale impactului asupra vieții private. Metodologia folosită pentru aceste evaluări se poate baza pe cadrul de evaluare a impactului asupra protecției vieții private și a datelor pe care Grupul de lucru „articolul 29" l-a adoptat la 12 ianuarie 2011 pentru aplicațiile RFID (*Privacy and Data Protection Impact Assessment Framework for RFID Applications*[32]). Dacă este indicat/fezabil, părțile interesate ar putea lua în considerare posibilitatea de a pune evaluările impactului asupra vieții private la dispoziția publicului larg. Pentru anumite ecosisteme specifice internetului obiectelor (cum ar fi orașele inteligente) ar putea fi elaborate cadre specifice de evaluare a impactului asupra vieții private.

- Numeroase părți interesate din domeniul internetului obiectelor au nevoie doar de date agregate, și nu de datele brute colectate de dispozitivelor IoT. Părțile interesate trebuie să șteargă datele brute imediat după ce au extras datele necesare pentru prelucrarea lor. În principiu, ștergerea ar trebui să aibă loc la cel mai apropiat punct de colectare a datelor brute (de exemplu pe același dispozitiv după prelucrare).

---

[29] În această privință, utilizarea unei abordări bazate pe așa-numitele politici *sticky* poate contribui la respectarea cadrului de protecție a datelor, prin încorporarea în datele înseși a unor informații despre condițiile și limitele de utilizare a acestora. Astfel, politicile respective ar putea stabili contextul de utilizare a datelor, scopurile, politicile privind accesul terților și o listă a utilizatorilor siguri.

[30] Recurgerea la servere proxy care permit protejarea vieții private ar putea constitui o modalitate de a oferi unei persoane vizate controlul efectiv asupra modului în care trebuie prelucrate datele atunci când interacționează cu senzori, dat fiind că acestor persoane li se dă posibilitatea să își exprime preferințele, inclusiv să își dea sau să și revoce consimțământul sau să recurgă la opțiunile de limitare a scopului. Dacă sunt susținute de un dispozitiv, cererile de date trebuie să respecte anumite politici predefinite care reglementează accesul la date aflate sub controlul persoanei vizate. Prin definirea unor perechi de politici și senzori, cererile de colectare a datelor de la senzor sau de acces la acestea care sunt lansate de terți pot fi autorizate, limitate sau pur și simplu respinse.

[31] Avizul nr. 02/2013 privind aplicațiile instalate pe dispozitivele inteligente (WP 202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_ro.pdf

[32] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

- Fiecare parte interesată din cadrul internetului obiectelor ar trebui să aplice principiile de luare în considerare a vieții private începând cu momentul conceperii și de respectare implicită a vieții private.

- Capacitarea adecvată a utilizatorilor este esențială în contextul internetului obiectelor. Persoanele vizate și utilizatorii trebuie să aibă posibilitatea de a-și exercita drepturile și deci de a fi „stăpâni” pe date în orice moment, conform principiului autodeterminării datelor.

- Metodele de furnizare a informațiilor, de oferire a dreptului de refuz și de cerere a acordului trebuie să fie cât mai simple cu putință. Mai precis, politicile de informare și de obținere a consimțământului trebuie să se axeze pe informații ușor de înțeles de către utilizator și nu ar trebui să se limiteze la o politică generală de respectare a vieții private, disponibilă pe site-ul operatorilor.

- Dispozitivele și aplicațiile ar trebui să fie astfel proiectate, încât să le informeze pe persoanele vizate, fie ele utilizatori sau nu , prin intermediul, de exemplu, al interfeței fizice a dispozitivului sau prin difuzarea unui semnal pe un canal fără fir.

6.2 **Fabricanții de sisteme de operare și de dispozitive**

- Fabricanții de dispozitive trebuie să îi informeze pe utilizatori cu privire la tipul de date colectate de senzori și prelucrate ulterior, la tipurile de date primite și la modul de prelucrare și combinare a acestor date.

- Fabricanții de dispozitive ar trebui să aibă capacitatea de a comunica cu toate celelalte părți interesate relevante de îndată ce o persoană vizată își revocă consimțământul sau se opune prelucrării datelor.

- Fabricanții de dispozitive trebuie să ofere opțiuni detaliate atunci când acordă acces la aplicații. Nivelul de detaliere nu ar trebui să se refere doar la categoria datelor colectate, ci și la momentul și frecvența de captare a informațiilor. Similar cu funcția „nu deranja” de pe telefoanele inteligente, dispozitivele IoT ar trebui să ofere opțiunea „nu colecta” pentru a programa sau a dezactiva rapid senzorii.

- Pentru a împiedica funcția de geolocalizare, fabricanții de dispozitive ar trebui să limiteze amprentarea dispozitivelor (*fingerprinting*) prin dezactivarea interfețelor fără fir atunci când nu sunt utilizate sau ar trebui să utilizeze identificatori aleatorii (cum ar fi adrese MAC aleatorii pentru scanarea rețelelor wifi) pentru a împiedica utilizarea unui identificator permanent la stabilirea poziției geografice a utilizatorului.

- Pentru a spori transparența și controlul exercitat de utilizatori, fabricanții de dispozitive ar trebui să le ofere acestora instrumente de citire, editare și modificare a datelor la nivel local, înainte de a fi transferate către un operator. În plus, datele cu caracter personal prelucrate de un dispozitiv ar trebui stocate într-un format care să permită portabilitatea datelor.

- Utilizatorii sunt autorizați să primească drept de acces la datele lor cu caracter personal. Ar trebui să li se pună la dispoziție instrumente care să le permită să își exporte cu ușurință datele într-un format structurat și utilizat în mod curent. Prin urmare, fabricanții de dispozitive ar trebui să pună la dispoziția utilizatorilor care doresc să obțină accesul la datele agregate și/sau datele brute pe care aceștia le stochează încă o interfață ușor de utilizat.

- Fabricanții de dispozitive ar trebui să pună la dispoziția utilizatorilor instrumente simple, care să pe aceștia îi avertizeze și să actualizeze dispozitivele atunci când se descoperă vulnerabilități de securitate. Atunci când un dispozitiv devine desuet și nu mai este actualizat, fabricantul dispozitivului ar trebui să îi avertizeze pe utilizatori și să se asigure că aceștia au cunoștință de faptul că dispozitivul nu va mai fi actualizat. Ar trebui informate, de asemenea, toate părțile interesate care ar putea fi afectate de respectiva vulnerabilitate.

- Fabricanții de dispozitive ar trebui să aplice principiul securității din stadiul conceperii și să rezerve anumite componente pentru principalele primitive criptografice.

- Fabricanții de dispozitive ar trebui să limiteze pe cât posibil cantitatea de date furnizate de dispozitive, prin transformarea datelor brute în date agregate direct pe dispozitiv. Datele agregate ar trebui să aibă un format standardizat.

- Spre deosebire de telefoanele inteligente, dispozitivelor IoT pot fi utilizate de mai multe persoane vizate sau chiar închiriate (cum ar fi locuințele inteligente). Ar trebui să existe o setare prin care să se facă distincția între mai multe persoane care utilizează același dispozitiv, astfel încât acestea să nu afle una despre activitățile alteia.

- Fabricanții de dispozitive ar trebui să coopereze cu organismele de standardizare și cu platformele de date pentru a sprijini un protocol comun pentru exprimarea preferințelor în ceea ce privește colectarea și prelucrarea datelor de către operatori, în special atunci când datele sunt colectate de dispozitive discrete.

- Fabricanții de dispozitive ar trebui să transfere competențe operatorilor locali și persoanelor împuternicite de aceștia la nivel local (*personal privacy proxies*) pentru a permite utilizatorilor să aibă o imagine clară a datelor colectate de dispozitivele lor și pentru a facilita stocarea și prelucrarea locală fără a fi nevoie ca datele să fie transmise către fabricantul dispozitivului.

6.3 **Dezvoltatori de aplicații**

- Avizele sau avertismentele ar trebui să fie concepute în așa fel încât să reamintească în mod frecvent utilizatorilor că se colectează date cu ajutorul senzorilor. În cazul în care dezvoltatorul de aplicații nu are acces direct la dispozitiv, aplicația ar trebui să transmită periodic utilizatorului o avertizare prin care să îl informeze că încă înregistrează date.

- Aplicațiile ar trebui să faciliteze exercitarea drepturilor de acces de către persoanele vizate, precum și modificarea și ștergerea datelor cu caracter personal colectate de dispozitivele IoT.

- Dezvoltatorii de aplicații ar trebui să ofere instrumente care să permită persoanelor vizate să exporte datele brute și/sau datele agregate într-un format standard și ușor de utilizat.

- Dezvoltatorii ar trebui să acorde o atenție specială tipurilor de date prelucrate și posibilității de a deduce din ele date sensibile cu caracter personal.

- Dezvoltatorii de aplicații ar trebui să aplice principiul reducerii la minimum a datelor. Atunci când scopul poate fi atins prin utilizarea de date agregate, dezvoltatorii nu ar trebui să acceseze datele brute. La un nivel mai larg, dezvoltatorii ar trebui să urmeze o abordare care ia în considerare viața privată începând cu momentul conceperii și să reducă volumul de date colectate la cantitatea necesară pentru furnizarea serviciului.

6.4 **Platformele sociale**

- Utilizatorilor ar trebui să li se ceară, încă din setările implicite ale aplicațiilor sociale bazate pe dispozitivele IoT, să verifice, să adapteze și să aleagă informațiile generate de dispozitivul lor înainte ca acestea să fie publicate pe platformele sociale.

- Informațiile publicate de dispozitivele IoT pe platformele sociale ar trebui, în mod standard, să nu devină publice sau să nu fie indexate de motoarele de căutare.

6.5 **Proprietarii de dispozitive IoT și alți destinatari**

- Consimțământul de utilizare a unui dispozitiv conectat și de prelucrare a datelor colectate de acesta trebuie să fie dat în cunoștință de cauză și în mod liber. Dacă utilizatorii decid să nu utilizeze dispozitivul sau un anumit serviciu, nu ar trebui ca aceştia să fie penalizați economic, și nici ca accesul acestora la funcțiile dispozitivului să fie restrâns.

- Persoana vizată ale cărei date sunt prelucrate în contextul unei relații contractuale cu utilizatorul unui dispozitiv conectat (cum ar fi un hotel, o societate de asigurări medicale sau o companie de închirieri auto) ar trebui să fie în măsură să administreze dispozitivul. Indiferent de existența unei relații contractuale, orice persoană vizată care nu este utilizator trebuie să aibă capacitatea de a-și exercita drepturile de acces și de opoziție.

- Utilizatorii dispozitivelor IoT ar trebui să le informeze pe persoanele vizate care nu sunt utilizatori și ale căror date sunt colectate cu privire la prezența dispozitivelor IoT și la tipul datelor colectate. Aceştia ar trebui, de asemenea, să respecte preferința persoanei vizate ca datele sale cu caracter personal să nu fie colectate de dispozitiv.

6.6 **Organismele de standardizare și platformele de date**

- Organismele de standardizare și platformele de date ar trebui să promoveze formate de date portabile și interoperabile care să fie clare și explicite, care să faciliteze transferurile de date între diferitele părți și care să ajute persoanele vizate să înțeleagă ce date sunt colectate efectiv cu privire la ele prin dispozitivele IoT.

- Organismele de standardizare și platformele de date nu ar trebui să se concentreze numai asupra formatului datelor brute, ci și asupra apariției unor formate de date agregate.

- Organismele de standardizare și platformele de date ar trebui să promoveze formatele de date care conțin cât mai puțini identificatori puternici, pentru a facilita anonimizarea corespunzătoare a datelor specifice internetului obiectelor.

- Organismele de standardizare ar trebui să elaboreze standarde certificate care să poată servi drept bază pentru garanțiile de securitate și de respectare a vieții private oferite persoanelor vizate.

- Organismele de standardizare ar trebuie să elaboreze protocoale suple de criptare și comunicare care să fie adaptate la caracteristicile specifice ale internetului obiectelor și care să garanteze confidențialitatea, integritatea, autentificarea și controlul accesului.