



Utilitate și riscuri în materia internetului obiectelor – provocări ale inteligenței artificiale

Călina JUGASTRU

Lucian Blaga University of Sibiu, Faculty of Law

Corresponding author emails: calina.jugastru@ulbsibiu.ro

Usefulness and Risks of the Internet of Things – Challenges of Artificial Intelligence

Abstract: In the context of the rule of law, artificial intelligence is at the forefront of challenges. Recently published in the Official Journal of the European Union (Series L/12.07.2024), the Artificial Intelligence Regulation amending a series of legal acts (Regulation (EU) 2024/1689) Artificial intelligence is a rapidly evolving family of technologies that contribute to a wide range of economic, environmental and societal benefits across the full spectrum of industries and societal activities. The upheavals at European and national level are visible, in recent years, in diverse matters: autonomous vehicles, autonomous drones, ChatGPT, robots (chatbots, deadbots, companion bots), deep-fake, blockchain, smart contracts, digital justice. Binding regulation was needed. From the applications as a whole, we are considering a subject that raises legal questions. The Internet of Things (Internet of Things, internet des objets) is a concept covering multiple realities. Connected objects are an integral part of the everyday world, and their use raises issues relating to inherent human rights, legal liability, the conclusion of contracts, etc. The benefits and risks are present, and the rules must be correlated. The new Artificial Intelligence Regulation is intimately linked to the General Data Protection Regulation (Regulation (EU) 2016/679). Smart cities is one of the concepts that evoke digitalization and interconnectedness in urban communities. Transportation, public services, tourism, sports, recreation, citizens' safety - all reflect the implications of artificial intelligence systems for efficiency and convenience in urban communities. At the same time, the massive processing of personal data opens up the possibility of security breaches (in collection, structuring, transfer). Quantified self offers solutions for self-awareness, through devices for measuring and quantifying activities. The willingness to share sensitive information (health data, genetic data, biometric data) on social networks or websites can facilitate the creation of personal databases by third parties (a priceless commodity due to the possibilities of consumer profiling). The common denominator of risk for all applications of artificial intelligence systems is big data. The sheer volume of data, processed at breakneck speed, is the foundation of systems that not only replicate what they have learned, but also have a degree of autonomy that can become difficult to manage. Both categories (utility/benefits - risks) are the subject of this study. Appropriate regulations are needed to determine the rules applicable to the legal regime of connected objects, preventing or mitigating the risks associated with them.

Keywords: Internet of Things, artificial intelligence, legal regime, utility of connected objects, risks of using connected objects

Citation suggestion: Jugastru, Călina. "Utilitate și riscuri în materia internetului obiectelor – provocări ale inteligenței artificiale." *Transilvania*, no. 11-12 (2024): 85-96.

<https://doi.org/10.51391/trva.2024.11-12.11>.



I. Preliminarii

Om și mașină – ființă și lucru – (sau) personalitatea juridică în derivă. La o primă vedere, intervenția acestei forme sofisticate a tehnologiilor (inteligența artificială), bulversează aliniamentele clasice ale dreptului, pe paliere multiple. Autonomia conferită sistemelor de inteligență artificială pune sub lupa interogațiilor capacitatea juridică (de folosință, de exercițiu, delictuală), răspunderea juridică ș.a. Nu vom enumera ramurile dreptului aflate sub impactul algoritmilor specifici inteligenței artificiale – în bună parte, internetul este privit ca un antecesor, iar inteligența algoritmică reprezintă o etapă superioară. De exemplu, *posibilitatea recunoașterii personalității juridice pentru*

anumite sisteme, cum sunt agenții conversaționali (roboții de tip *chatbots* și *deadbots*¹), este dezbătută în doctrina juridică². *Normele de drept civil privind robotica* (incluse în Rezoluția Parlamentului European din 2017) recomandă „crearea unui statut juridic specific pentru roboți, astfel încât cel puțin cei mai sofisticați roboți autonomi să poată avea un statut de persoană electronică responsabilă pentru repararea prejudiciilor pe care le cauzează și să poată fi aplicată eventual personalitatea electronică în cazurile în care roboții iau decizii autonome sau interacționează independent, în alt fel, cu terți” (pct. 59 lit. f)³. De asemenea, *protecția drepturilor subiective cunoaște particularități atunci când intră în ecuație algoritmi smart*. La confluența aspectelor umane, sociale și tehnice, „Sistemele IA nu ar trebui să subordoneze, să constrângă, să inducă în eroare, să manipuleze, să condiționeze sau să direcționeze prin spirit de turmă oamenii în mod nejustificat. În schimb, sistemele IA ar trebui să fie proiectate astfel încât să sporească, să completeze și să permită competențele cognitive, sociale și culturale ale oamenilor”⁴.

În **ansamblul reglementărilor statului de drept, inteligența artificială se situează pe linia provocărilor**. Definită ca „domeniu interdisciplinar teoretic și practic al cărui scop este înțelegerea mecanismelor de cunoaștere și reflecție, precum și imitarea acestora de către un dispozitiv *hardware* și *software*, în scopul de a asista sau de a înlocui activitățile umane”⁵, inteligența artificială nu are antecedente normative. Anul 2024 a concretizat primul regulament european care are ca obiect utilizarea sistemelor de inteligență artificială (principii, aplicații, interdicții, excepții, cooperarea autorităților competente). Conform Regulamentului (UE) 2024/1689, „*sistemul de inteligență artificială*” este un sistem bazat pe o mașină, „conceput să funcționeze cu diferite niveluri de autonomie, care poate prezenta adaptabilitate după implementare și care, urmărind obiective explicite sau implicite, deduce, din datele de intrare pe care le primește, modul de generare a unor rezultate precum previziuni, conținut, recomandări sau decizii care pot influența mediile fizice sau virtuale (art. 3 pct. 1)⁶. O particularitate a sistemelor constă în posibilitatea de a reproduce abilități care ar presupune „inteligență” la ființele umane (raționament, autonomie, creativitate ș.a.). Tehnologiile de inteligență artificială utilizează învățarea automată (care presupune alimentarea sistemelor informatice cu exemple, date și experiență, așa încât acestea să fie capabile să îndeplinească sarcini în mod inteligent). Gradul de autonomie cu care sunt dotate, permite sistemelor să adopte decizii, să acționeze stabilindu-și propriile obiective, adaptându-se la condițiile locale datorită informațiilor transmise de senzorii lor sau de asimilarea datelor actualizate. Proiectanții acestor sisteme nu fac decât să determine parametrii inițiali și obiectivul general pe care sistemul trebuie să îl atingă într-un mod optim. Sistemele de învățare automată iau apoi decizii în mod independent, optând pentru cea mai bună alternativă în moduri care nu au fost programate în prealabil și fără nicio intervenție umană. În mod continuu și iterativ, aceste sisteme sisteme învață din mediul lor, care la rândul său este adesea schimbător și dezordonat, ceea ce poate

1. Primul termen (*chatbots*) desemnează sisteme digitale care au aptitudinea de a interacționa cu utilizatorii în limbaj uman, scris și oral (*smartphone*-uri, difuzoare conectate, mașini, *site-uri web* etc.). Se bazează pe aplicația dezvoltată de Google sub denumirea «LaMDA» (*Language Model for Dialogue Applications*) și sunt, de regulă, integrate unor platforme digitale sau unor roboți. Terminologia *deadbots* desemnează agenți conversaționali care imită modul în care a vorbit sau a scris o persoană decedată. Pe baza unor informații colectate anterior (fotografii, înregistrări audio/video), un *deadbot* poate să imite limbajul sau comportamentul celui trecut în neființă. În mod obișnuit, agentul conversațional nu repetă doar datele de instruire, ci are și capacitatea de a genera enunțuri noi, care nu au fost rostite de către defunct. Unele dintre aceste sisteme pot avea un dialog realist, eventual îmbunătățit de capacitatea *chatbotului* de a simula emoțiile. Interlocutorul uman poate avea impresia că este în prezența persoanei imitate, chiar dacă este informat că, în cauză, este vorba de o mașină.

2. Tezele favorabile personificării sistemelor de inteligență artificială sunt expuse în Jean-Michel Bruguière, Bérengère Gleize, *Droit des personnes* (Paris: Lefebvre Dalloz, 1^{re} éd., 2023), 225-227.

3. A se vedea *Normele de drept civil privind robotica*. Rezoluția Parlamentului European din 16 februarie 2017 conținând recomandări adresate Comisiei referitoare la normele de drept civil privind robotica, publicate în JO C 252/239/18.07.2018. Pentru un tablou al reglementării la nivel european a se vedea, Maria Castillo, „L'Union européenne: vers la maîtrise de l'intelligence artificielle?”, *Cahiers de la recherche sur les droits fondamentaux*, nr. 21 (2023): 99-107.

4. *Orientări în materie de etică pentru o inteligență artificială (IA) fiabilă*, Grupul de experți la nivel înalt privind inteligența artificială, document publicat în 8.04.2019, p. 13-14, disponibil pe pagina <https://op.europa.eu/ro/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1> (accesat la 20.06.2024).

5. *Vocabulaire de l'intelligence artificielle (liste de termes, expressions et définitions adoptés)*, JORF n° 0285/9.12.2018.

6. Regulamentul (UE) nr. 2024/1689 de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 a fost publicat în JO Seria L/12.07.2024. Noul Regulament intră în vigoare la 20 de zile de la publicare și se va aplica în etape.



face ca funcționarea să fie instabilă și imprezvizibilă⁷.

Dintre aplicațiile inteligenței artificiale, avem în vedere **internetul obiectelor** (*Internet of Things*, *internet des objets*) – un concept care acoperă realități diverse. Dacă internetul a revoluționat sectoarele vieții sociale și a antrenat legiferări inedite, inteligența artificială, respectiv, internetul obiectelor, depășesc acest prag și inițiază un univers interconectat. Pe baza unor tehnologii specifice, obiectele sunt conectate (cu utilizatorii și unele cu altele), dobândind o anumită autonomie în primirea și transmiterea informațiilor. Cotidian, recurgem la obiecte conectate, iar proiectele inițiate de guvernanți tind spre **comunitățile urbane smart** (*smart cities*). Dacă mapamondul obiectelor conectate va fi o țesătură de orașe cu elemente *smart*, digitalizarea poate fi regăsită și la nivel individual. Competiția cu sinele (și cu alții) pare a nu cunoaște limite – astfel că evaluarea propriilor activități, rezultate, performanțe se îndreaptă spre perfecțiune. *Quantified self* (*life-logging*, *self tracking*) este un concept ce redă ideea măsurării/cuantificării (propriului corp) prin intermediul obiectelor conectate (ceasuri, brățări conectate, podometre etc.). Această tehnică modernă este mai mult decât o simplă constatare a valorilor sau rezultatelor unei activități – se adaugă analiza și partajarea, de regulă, în cadrul rețelelor de socializare. Ceea ce trebuie imediat precizat este că auto-măsurarea caracteristicilor fizice este indisolubil asociată prelucrării datelor cu caracter personal. Comisia națională pentru informatică și libertăți din Franța (CNIL) a recomandat utilizatorilor să nu își decline identitatea prin instrumentele *quantified self*, iar, dacă recurg la dispozitive medicale conectate, să solicite avizul cadrelor medicale.

Vom exemplifica, în registrul beneficiilor și al riscurilor, cele două componente ale internetului obiectelor. *Smart cities* constituie viitorul digitalizării citadine, iar *quantified self* este omniprezent. Prealabil, vom menționa caracteristicile esențiale ale internetului obiectelor.

II. Internetul obiectelor – noțiune, caracteristicile obiectelor conectate

O **definiție** „specializată” a fost formulată de Uniunea Internațională a Telecomunicațiilor (agenția Organizației Națiunilor Unite pentru telecomunicații și tehnologii ale informației și comunicațiilor). Internetul obiectelor este o „infrastructură globală pentru societatea informațională, care furnizează servicii avansate prin interconectarea obiectelor (fizice sau virtuale) utilizând tehnologiile informației și comunicațiilor interoperabile existente sau în curs de evoluție”⁸. Internetul obiectelor este rezultanta procesului de combinare a tehnologiilor informației: orașele inteligente, vehiculele conectate, rețele de senzori fără fir (WSN), *cloud computing*, *big data*, *blockchains*. „Obiectul” este o mașină fizică sau virtuală, care: este *inteligentă* – are o anumită capacitate de calcul și de memorie; este *autonomă*, întrucât poate prelucra date și, uneori, chiar lua decizii fără intervenție umană; este *aptă a fi conectată* la orice alt obiect într-un mod flexibil și transparent. Menționăm **caracteristicile** care configurează internetul obiectelor. *Senzorii sunt proiectați pentru a facilita comunicarea (între obiecte, între obiecte și persoane)*. Miliarde de senzori care dau viață internetului obiectelor constituie o infrastructură încorporată în dispozitivele cotidiene. Sunt obiecte destinate 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”⁹. Apoi, *obiectele conectate prelucrează masiv date cu caracter personal*. Explicația este la îndemână, căci acesta este rostul internetului obiectelor – 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 analiza în mod specific comportamentul acestuia»¹⁰. Utilizatorul este identificat sau este identificabil, astfel că datele prelucrate întrunesc cerințele cerute de Regulamentul (UE)

7. A se vedea, „*Étude sur les incidences des technologies numériques avancées (dont l’intelligence artificielle) sur la notion de responsabilité, sous l’angle des droits humains*”, Préparée par le Comité d’experts sur les dimensions des droits de l’homme dans le traitement automatisé des données et les différentes formes d’intelligence artificielle (MSI-AUT), Conseil de l’Europe, septembre 2019 (<https://edoc.coe.int/en/artificial-intelligence/8025-responsabilite-et-ia.html>, accesat la data de 20.05.2024).

8. Union Internationale des Télécommunications, Recommandation UIT-T Y.2060, *Série Y: infrastructure mondiale de l’information, protocole internet et réseau de prochaine generation – Cadre général et modèles architecturaux fonctionnels*, 6 (2012): 1.

9. Grupul de lucru „Articolul 29” pentru protecția datelor, *Avizul nr. 8/2014 cu privire la evoluțiile recente din sfera internetului obiectelor*, 1471/14/RO WP 223, p. 4, disponibil pe pagina dataprotection.ro, accesat la data de 20.05.2024.

10. Grupul de lucru „Articolul 29” pentru protecția datelor, *Avizul nr. 8/2014 cu privire la evoluțiile recente din sfera internetului obiectelor*, 1471/14/RO WP 223, *loc. cit.*

2016/679 pentru a fi calificate ca atare. *Date cu caracter personal* înseamnă orice informații privind o persoană fizică identificată sau identificabilă¹¹ („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume¹², un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale” (art. 4 pct. 1). *Datele sensibile* sunt colectate, stocate, structurate prin intermediul obiectelor conectate (de exemplu dispozitive medicale conectate, obiecte utilizate în biometrie) și sunt guvernate de regula de principiu a interdicției de prelucrare¹³. Astfel, informațiile care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate, datele genetice, datele biometrice pentru identificarea unică a unei persoane fizice, datele privind sănătatea, datele privind viața sexuală sau orientarea sexuală ale unei persoane fizice pot fi prelucrate numai dacă se încadrează în excepțiile legale (art. 9 alin. 1)¹⁴.

Aceste câteva considerații ne introduc în sfera divizată, a utilităților și riscurilor obiectelor conectate. Multiplele destinații – de la cotidianul domestic, vehiculele autonome, *smart contracts*, la aplicațiile de monitorizare a sănătății și a stilului de viață, conferă utilitate. Riscurile sunt dificil de inventariat. Desprindem, într-o tușă de generalitate, pericolele potențiale, la adresa vieții private și a datelor cu caracter personal. Dintre componentele internetului obiectelor, avem în vedere comunitățile urbane *inteligente* (identificate prin terminologia *smart cities*)¹⁵ și sinele cuantificat (desemnat prin *quantified self*).

III. *Smart cities (villes numériques)*

Noțiune care revendică un loc în contextul internetului obiectelor, *smart cities* a primit definiții apropiate în doctrină¹⁶. Studiile efectuate la nivelul comunităților care au implementat instrumente specifice, relevă axele esențiale¹⁷: *smart economy* (competitivitate – spirit inovator, antreprenariat, productivitate, flexibilitatea pieței muncii); *smart people* (capital social și uman – nivelul de calificare, învățarea permanentă, pluralitatea socială și etnică, creativitate, participare la viața publică); *smart governance* (participare – participare la procesul decizional, servicii publice, guvernare transparentă, strategii politice și perspective); *smart mobility* (transporturi, TIC – posibilități de acces local și național, infrastructură TIC); *smart environnement* (resurse naturale – protecția mediului, resurse durabile); *smart living* (calitatea vieții – sănătate, securitatea individului, facilități pentru educație, atractivitatea turistică). Beneficiile pe care tehnologiile digitale le oferă comunităților urbane sunt de natură a umbri uneori riscurile. Tentația eficienței maxime și a economiilor drastice ridică la rang de prioritate implementarea unor soluții – citirea la distanță a contoarelor, parcările inteligente, economisirea resurselor de apă, colectarea deșeurilor și iluminatul stradal realizate pe baza senzorilor

11. Lucian Marcu, „Întâmpinarea în procesul civil I. Conținutul întâmpinării și sancțiunile aplicabile în cazul nerespectării dispozițiilor legale în materie”, *Acta Universitatis Lucian Blaga*, Seria Iurisprudentia, nr. 2 (2017): 77.

12. Numele este atributul de identificare al persoanei fizice care îi conferă acesteia dreptul de a fi individualizată prin anumite cuvinte, în familie și în societate. Ca structură, numele cuprinde numele de familie (numele patronimic) și prenumele (numele de botez). A se vedea, pentru detalii, Gina Orga-Dumitriu, *Instituții de drept public și privat* (București: C.H. Beck, 2011), 87.

13. Datele sensibile (ale consumatorilor) sunt o resursă și pentru companiile care desfășoară afaceri consistente pe platforme *on-line*. Este cazul platformei Amazon, care se pare că utilizează informații sensibile cu privire vânzătorii independenți (pentru care pune la dispoziție piață de desfacere), produse și tranzacții – informații rezultate în cadrul procedurilor de investigare la nivel european. Pentru detalii, cu privire la demersurile respective, a se vedea, Lucia Irinescu, „Noi provocări în era digitală. Politica de concurență”, *Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași*, tomul LXV, Științe Juridice (2019): 54

14. Pentru datele cu caracter personal necesare derulării procedurii judiciare privind cererile de valoare redusă, a se vedea, Lucian Marcu, „Întâmpinarea în procesul civil II. Excepții de la regula obligativității întâmpinării”, *Acta Universitatis Lucian Blaga*, Seria Iurisprudentia, nr. 1 (2018): 102-114.

15. Hervé Rannou, „L’Internet des objets: d’une vision globale à des applications bien plus éparées”, *Annales des mines – réalités industrielles*, nr. 2 (2013): 70-118.

16. Exemplificativ: „concept de planificare urbană care crește eficiența gestionării urbane prin introducerea unui complex de tehnologii informatice avansate și a internetului obiectelor (IoT)” («Live smart, go digital: biometric identification in the „Smart City” concept», material disponibil pe pagina <https://recfaces.com/articles/biometric-identification-in-the-smart-city-concept>, accesat la 20.06.2024);

17. Rudolf Giffinger, Christian Fertner, Hans Kramar, Robert Kalasek, Natasa Pichler-Milanović, Evert Meijers, *Smart cities – Ranking of European medium-sized cities*, Final Report, Centre of Regional Science (SRF). Vienna University of Technology, 2007, 10-12.



conectați, asigurarea securității comunității (împotriva conduitei care încalcă legea) prin intermediul instrumentelor de videosupraveghere și identificare biometrică. Dintre situațiile care îmbină aspectele pozitive și riscurile, *Strava Metro* și biometria sunt reprezentative pentru comunitățile urbane *smart*.

1. Exemplul *Strava Metro*

Un exemplu de beneficii și riscuri este *Strava Metro*. Rețea socială online pentru cicliști și atleți, *Strava* funcționează ca aplicație pentru mobil și *site web*, permițând utilizatorilor să urmărească activitățile membrilor rețelei (plimbări, drumeții, curse) și să încarce propriile activități¹⁸. Prin intermediul aplicației sunt înregistrate distanța, timpul, viteza medie și traseul (traectoria GPS) pentru fiecare activitate, iar utilizatorii pot adăuga informații text (titluri și etichete pentru a-și descrie călătoriile). Din perspectiva *smart cities*, această aplicație este benefică din multe puncte de vedere. Întâi de toate, *Strava* permite colectarea rapidă a informațiilor detaliate și cartografierea traseelor ciclistice – împrejurare care presupune reducerea costurilor și a timpului de introducere manuală a datelor. De asemenea, prelucrarea informațiilor generate de utilizatori vizează optimizarea infrastructurii, echipamentelor destinate sportivilor, precum și asocieri între ciclism și sănătate¹⁹. Aplicația are însă și alte utilități. Datele sunt agregate și permit extragerea informațiilor privind nivelul de poluare a aerului. Incontestabilele beneficii pentru sănătate ale mersului cu bicicleta (datorită activității fizice) sunt însoțite uneori de riscuri – poluarea aerului, accidentele și zgomotul. Analizele efectuate în comunitățile urbane permit decelarea nivelului de poluare a aerului (de exemplu, dacă depășește limitele impuse de Organizația Mondială a Sănătății) și constituie un sprijin pentru factorii decizionali ai *smart cities* în soluționarea problemelor de sănătate publică și de mediu²⁰. Succesul *Strava Metro* se corelează cu breșe de securitate care, în decursul timpului, au afectat infrastructura militară. În anul 2017, *Strava* a generat o hartă termică (punctele luminoase de pe hartă indicau zonele cu activitate fizică intensă). Astfel, prin căutarea regiunilor luminoase pe harta *Strava*, a devenit posibilă localizarea unor instalații ale armatei americane (unele secrete), deoarece o serie de utilizatori erau membri ai armatei. Traseul soldaților care desfășurau exerciții fizice a dezvăluit locația bazei militare. Informațiile au fost disponibile pe pagina publică de internet: prin mărirea hărții termice, a fost posibil să se obțină numele complet și activitățile utilizatorilor individuali staționați la anumite baze militare²¹.

2. Identificarea biometrică

Reglementarea biometriei era necesară, la nivel european. Întâi de toate, consecințele asociate

18. A se vedea, Yeran Sun, Amin Mobasher, „Utilizing Crowdsourced Data for Studies of Cycling and Air Pollution Exposure: A Case Study Using Strava Data”, *International Journal of Environmental Research and Public Health*, nr. 3 (2017): 274. *Strava* are o bază de utilizatori mai mare decât *site-uri* similare, precum MapMyRide (Under Armour, Baltimore, MD, SUA), MapMyRun (Under Armour, Baltimore, MD, SUA) sau RideWithGPS (Ride with GPS, Portland, OR, SUA).

19. Ben Jesticoa, Trisalyn Nelsona, Meghan Wintersb, „Mapping ridership using crowdsourced cycling data”, *Journal of Transport Geography*, vol. 52 (2016): 90–97; Kristiann C. Heesch, Bruce James, Tracy L. Washington, Kelly Zunig, Matthew Burke, „Evaluation of the Veloway: A natural experiment of new bicycle infrastructure in Brisbane, Australia”, *Journal of Transport & Health*, nr. 3 (2016): 366–376; Greg P. Griffin, Jungfeng Jiao, „Where does bicycling for health happen? Analysing volunteered geographic information through place and plexus”, *Journal of Transport & Health*, nr. 2 (2015): 238–247. Toate lucrările sunt citate după Yeran Sun, Amin Mobasher, „Utilizing Crowdsourced Data for Studies of Cycling and Air Pollution Exposure: A Case Study Using Strava Data”, 274.

20. Pentru exemplificare, la nivelul comunităților din Glasgow (Regatul Unit) și El Paso (Texas), a se vedea, Yeran Sun, Amin Mobasher, 274; Lee Kyuhyun, N. Sener Ipek, „Understanding Potential Exposure of Bicyclists on Roadways to Traffic-Related Air Pollution: Findings from El Paso, Texas, Using Strava Metro Data”, 1-20.

21. Cu privire la aceste aspecte, a se vedea, Susan Landau, Patricia Vargas Leon, „Reversing Privacy Risks: Strict Limitations on the Use of Communications Metadata and Telemetry Information”, *Colorado Technology Law Journal*, nr. 2 (2023): 283; Marianne Gluckert Smith, „Tracing Property Interests: How Mandatory COVID-19 Contact Tracing Conflicts with the Maryland Constitution and Trade Secret Law”, *University of Baltimore Law Forum*, nr. 2 (2022): 202-203; William Osei-Bonsu, Aviel Stein, Michael Boswell, „The Current Ethical and Regulatory Status of the Internet of Medical Things (IoMT) and the Need of a New IoMT Law”, *The Journal of Healthcare Ethics & Administration*, nr. 2 (2018): 35; Eric Hinsdale, Abby Clobridge, „The Dark Side of Open Data”, *Information Today*, noiembrie/decembrie (2018), disponibil pe pagina <https://www.infotoday.com/OnlineSearcher/Articles/The-Open-Road/The-Dark-Side-of-Open-Data-128477.shtml>, accesat la data de 20.06.2024; Richard Pérez-Peña, Matthew Rosenberg, „Strava Fitness App Can Reveal Military Sites, Analysts Say”, *The New York Times*, 29.01.2018 (<https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html>, accesat la data de 20.06.2024).

prelucrării datelor personale sensibile, trebuiau strict prevăzute, într-un act normativ cu caracter obligatoriu. Prin urmare, regulile ce guvernează materia au fost incluse în primul act normativ care reglementează inteligența artificială, publicat în data de 12 iulie 2024. Regulamentul (UE) 2024/1689 menționează că *identificarea biometrică* presupune recunoașterea automată a unor trăsături umane fizice, fiziologice și comportamentale, cum sunt: fața, mișcările ochilor, forma corpului, vocea, intonația, mersul, postura, frecvența cardiacă, tensiunea arterială, mirosul, particularitățile de tastare – cu scopul de a stabili identitatea unei persoane comparând datele biometrice²² ale respectivei persoane cu date biometrice stocate într-o bază de date de referință, indiferent dacă persoana în cauză și-a dat sau nu consimțământul. *Verificarea biometrică* implică verificarea automată, pe baza unei comparații între două seturi de date, inclusiv autentificarea, a identității persoanelor fizice prin compararea datelor biometrice ale acestora cu datele biometrice furnizate anterior (art. 3 pct. 35, 36).

La capitolul „Practici interzise în domeniul IA” sunt menționate: *introducerea pe piață, punerea în funcțiune în acest scop specific sau utilizarea unor sisteme de IA care creează sau extind bazele de date de recunoaștere facială prin extragerea fără scop precis a imaginilor faciale de pe internet sau de pe înregistrările TVCI* (art. 5 par. 1 lit. e); *introducerea pe piață sau punerea în funcțiune în acest scop specific sau utilizarea de sisteme de clasificare biometrică*, ce clasifică în mod individual persoanele fizice pe baza datelor lor biometrice pentru a deduce sau a intui rasa, opiniile politice, apartenența la un sindicat, convingerile religioase sau filozofice, viața sexuală sau orientarea sexuală ale persoanelor respective – această interdicție nu se referă la etichetarea sau filtrarea seturilor de date biometrice obținute în mod legal, cum ar fi imaginile, pe baza datelor biometrice sau la clasificarea datelor biometrice în domeniul aplicării legii (art. 5 par. 1 lit. g); *utilizarea sistemelor de identificare biometrică în timp real în spații accesibile publicului în scopul aplicării legii*²³.

Utilitatea biometriei (la distanță, în timp real, în spații accesibile publicului) rezultă din reglementarea celor trei *excepții*: căutarea în mod specific a anumitor victime ale răpirii, traficului de persoane sau exploatării sexuale a persoanelor, căutarea persoanelor dispărute; prevenirea unei amenințări specifice, substanțiale și iminente care vizează viața sau siguranța fizică a persoanelor fizice sau a unei amenințări reale și prezente sau reale și previzibile de atac terorist; localizarea sau identificarea unei persoane suspectate de săvârșirea unei infracțiuni, în scopul desfășurării unei investigații penale sau al urmăririi penale sau al executării unor sancțiuni penale pentru infracțiunile arătate expres, pasibile (în statul membru respectiv) de o pedeapsă privativă de libertate sau o măsură de siguranță privativă de libertate pentru o perioadă de cel puțin patru ani.

Se poate observa, excepțiile privesc obiective asociate garantării vieții și integrității persoanelor²⁴. Așteptările cetățenilor în direcția siguranței personale, protecției vieții, integrității, protecției bunurilor – prin intermediul unor tehnici precise, sunt legitime. Odată cu beneficiile, riscurile trebuie cunoscute și gestionate. Din perspectiva *smart cities*, cel mai comod temei juridic al prelucrării datelor este consimțământul persoanei vizate. Se încadrează în această ipoteză, de pildă, utilizarea tehnicilor biometrice la accesul în mijloacele

22. *Datele biometrice* sunt date cu caracter personal rezultate în urma unor tehnici de prelucrare specifice, referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice (art. 3 pct. 34 din Regulamentul privind inteligența artificială și art. 4 pct. 14 din Regulamentul general privind protecția datelor). Aceste date fac posibile autentificarea, identificarea, clasificarea persoanelor fizice, recunoașterea emoțiilor acestora.

23. *Sistemul de identificare biometrică la distanță în timp real* presupune capturarea datelor biometrice, compararea și identificarea – operațiuni care au loc fără întârzieri semnificative și includ nu numai identificarea instantanee, ci și întârzieri scurte limitate pentru a se evita eludarea. *Spațiu accesibil publicului* înseamnă orice loc fizic aflat în proprietate publică sau privată, accesibil unui număr nedeterminat de persoane fizice, indiferent dacă se pot aplica anumite condiții de acces și indiferent de potențiale restricții de capacitate (art. 3 pct. 42, 44 din Regulamentul privind inteligența artificială).

24. Pentru fiecare utilizare, în scopul aplicării legii, a sistemului de identificare biometrică la distanță în timp real în spațiile accesibile publicului, se impune obținerea autorizației prealabile emisă de autoritatea judiciară/autoritatea administrativă independentă a cărei decizie are efect obligatoriu în statul membru de utilizare. Regulamentul european detaliază procedura de obținere a autorizației și condițiile în care utilizarea sistemului poate începe fără autorizație, în caz de urgență justificată.



de transport în comun²⁵, în aeroporturi, în cadrul serviciilor publice (identificare prin amprenta digitală, prin elementele caracteristice ale mâinii, identificarea vocală, identificarea facială, scanarea retinei), la securizarea mijloacelor de plată²⁶, acordarea îngrijirilor medicale de urgență, intervenții în cazul dezastrelor (geolocalizarea are rol major în ultimele două situații). Alături de metodele clasice de identificare, a fost propusă biometria cardiacă prin ECG. În contextul comunităților inteligente, se arată că, identificarea cardiacă depășește erorile constatate la amprenta digitală sau scanarea facială. Biometria clasică întâlnește obstacole ce conduc la denaturarea rezultatelor – de exemplu, transpirația care afectează degetele, culoarea neagră a pielii, anumite handicapuri fizice, temperatura aerului (recunoașterea pe baza amprentei digitale produce erori sub -10 grade Celsius), gemenii nu pot fi identificați în mod unic. În schimb, bătăile inimii, forma și dimensiunea acestui organ sunt unice pentru fiecare individ. Biometria cardiacă poate fi utilizată pentru aplicații de înaltă securitate datorită caracteristicilor de detectare a prezenței care duce la autentificarea individului în timp real²⁷.

Utilizarea biometriei în smart cities este asociată unui nivel de risc inacceptabil sau risc ridicat pentru viața privată. Sintagme precum „dreptul de a fi lăsat singur” sau „dreptul de a fi lăsat în pace” au devenit locuri comune de discuție. Consacrat în legea fundamentală română, dreptul la viață privată²⁸ are un statut aparte în contextul drepturilor personalității și – mergând mai departe – are forme specifice de manifestare în mediul digital. Esența vieții private se suprapune unui sector personal în care nimeni nu poate pătrunde fără acordul celui în cauză, o sferă ce reunește, în principal, relațiile de familie²⁹, viața sentimentală, starea de sănătate, intimitatea căminului etc. În perimetrul privat, subiectul are controlul deplin al informațiilor, deciziilor și acțiunilor care îl privesc; într-o anumită măsură, viața privată include și dreptul individului de a stabili și dezvolta relații cu semenii săi³⁰.

Prezența în spațiul public nu are semnificația renunțării la protecția aspectelor care sunt de resortul vieții private. De exemplu, tehnicile de identificare biometrică la distanță (în timp real, a persoanelor fizice în spațiile accesibile publicului, în scopul aplicării legii) prezintă riscul intruziunii, afectând viața privată a unui număr de persoane, pot inspira un sentiment de supraveghere constantă și pot descuraja (indirect) exercitarea libertății de întrunire și a altor drepturi fundamentale. În preambulul noului Regulament european se arată că, inexactitățile tehnice ale sistemelor de inteligență artificială destinate identificării biometrice la distanță a persoanelor fizice pot conduce la rezultate distorsionate de prejudecăți și pot avea efecte discriminatorii. Astfel de rezultate posibile sunt relevante, cu precădere în ceea ce privește vârsta, etnia, rasa, sexul sau dizabilitatea. În plus, caracterul imediat al impactului și posibilitățile limitate de a efectua verificări sau corecții suplimentare în ceea ce privește utilizarea unor astfel de sisteme care funcționează în timp real implică riscuri sporite pentru drepturile și libertățile persoanelor vizate în contextul activităților de aplicare a legii sau impactate de acestea (considerentul 32).

De exemplu, proiectul unui sistem de supraveghere video „inteligent”, destinat orașului argentinian Tigre în 2011, a vizat scăderea ratei criminalității (rată ridicată, în pofida unei populații nu foarte numeroase, aproximativ 31 de mii de persoane). Camerele biometrice au fost capabile nu numai să

25. O altă facilitate este optimizarea transportului în comun. Se arată că, instalarea unei camere de supraveghere video cu tehnologie de recunoaștere facială în interiorul vehiculului, permite stabilirea numărului pasagerilor. Cu ajutorul acestor date, pot fi determinate cele mai aglomerate rute și pot fi calculate intervalele exacte ale orelor de vârf. O astfel de analiză sprijină îmbunătățirea programului de transport (numărul de plecări pe linii poate fi modificat, în funcție de traseu). Utilizarea supravegherii video inteligente și a porților electronice cu tehnologie de recunoaștere facială în aeroporturi și gări poate accelera (cu aproximativ 30%) parcurgerea formalităților premergătoare transportului. Identificarea biometrică poate fi utilizată în toate etapele de control, de la livrarea bagajelor până la controlul vamal.

A se vedea, «Live smart, go digital: biometric identification in the „Smart City” concept», *op. cit.*

26. Cu titlu de exemplu, sistemele de plăți pe bază de identificare facială funcționează în China (Alipay și WeChat Pay), California (PopId). A se vedea, pentru detalii privind funcționarea plăților biometrice, Menjun Tao, Richard Jiang, Carolyn Downs, „Ethics of Face Recognition in Smart Cities Toward Trustworthy AI”, în *Big Data Privacy and Security in Smart Cities: Advanced Sciences and Technologies for Security Applications* (Springer International Publishing, 2022), 23-52.

27. Rohit Rastogi, „Using ECG Authentication for Biometrics in Smart Cities”, *International Journal of Systems and Software Security and Protection*, nr. 1 (2023), p. 3.

28. Cu privire la interpretarea sintagmei „drept la viață privată”, în contextul Convenției europene a drepturilor omului, art. 8, a se vedea, Frédéric Sudre, *Drept european și internațional al drepturilor omului* (Iași: Polirom, 2006), 312-342.

29. Cu privire la accepțiunea restrânsă și la sensul extins al termenului „familie”, a se vedea. C.C. Hageanu, *Dreptul familiei*, Ediția a 3-a revizuită și adăugită (București: Hamangiu, 2023), 7-9.

30. În acest sens, Eliodor Tanislav, „Ocrotirea penală a dreptului la intimitate”, *Revista de drept penal*, nr. 3 (1998), p. 48.

recunoască fețele, ci și să detecteze comportamentele suspecte. Informațiile erau transmise organelor de poliție în timp real, iar efectul a fost impresionant – numărul furturilor de mașini din oraș a scăzut cu 80%. Informațiile colectate prin sistemul video biometric au constituit baza „hărții infracționale” a orașului, ceea ce a condus la asigurarea unei supravegheri riguroase în zone considerate periculoase. Integrarea funcției de recunoaștere facială are eficiență sporită și automatizează procesul de identificare. O fotografie a suspectului/infractorului permite a se obține instantaneu informații cu privire la locațiile și traseul pe care le-a parcurs în oraș, precum și conexiunile sociale (persoanele cu care s-a întâlnit, traseul acestora)³¹. Supravegherea video în *smart cities* vizează, îndeosebi, mulțimile de oameni, în transportul public, pe stadioane, în marile centre comerciale, în cadrul obiectivelor turistice. Concluzia se impune, de îndată: intruziunea în viața privată persistă, cu prilejul unei monitorizări „în masă” (la nivelul anului se estima existența unui număr de 657 de camere pe kilometru pătrat în Chennai, 399 în Londra, 277 în Beijing și 254 în Paris)³².

Unul dintre instrumentele de poliție predictivă, bazat pe colectarea masivă de date și supravegherea în masă a fost evocat în presă, în raport cu rata crescută a criminalității în orașul New Orleans. A fost în discuție *software*-ul Palantir, care se presupunea că poate identifica persoanele cu risc ridicat de implicare în acte de violență (prin analiza conjugată a rapoartelor poliției, a rețelelor sociale și a altor baze de date, inclusiv a jurnalelor/evidențelor telefonice din închisori). Articolul publicat în *The Verge*, în 2018, menționa o listă de 3.900 de persoane considerate a fi cele mai expuse riscului. Se arăta, la acea vreme, că cei în cauză aveau posibilitatea de a se înscrie în programele sociale specific (pentru reeducare) sau să facă obiectul unei supravegheri sporite din partea organelor de poliție³³.

IV. Sinele cuantificat (*quantified self, auto-mesure connectée*)

Ideea măsurării, cuantificării, raportării la standarde sau la performanțele altora nu este inedită. Dimpotrivă, este anterioară atât obiectelor conectate, cât și *web*-ului. Forumurile de discuții, de pildă, continuă să fie zone în care utilizatorii dezbate propriile experiențe adesea de natură medicală, solicită și oferă recomandări, sugestii. Inițial, auto-măsurarea era efectuată manual, însă, utilizarea instrumentelor de măsurare conectate la o rețea informatică, a sporit eficiența rezultatelor. Auto-măsurarea conectată este parte integrantă a internetului obiectelor. Ea reprezintă practica utilizării obiectelor conectate pentru a măsura variabile fiziologice legate de alimentația, activitatea fizică sau somnul unei persoane³⁴. Termenul *sine cuantificat* se referă la *practica de măsurare a propriei persoane*, o mișcare originară în California, ce implică mai buna cunoaștere a propriei persoane prin măsurarea datelor referitoare la corpul și activitățile proprii³⁵. Ceea ce inovează auto-măsurarea conectată este utilizarea internetului obiectelor pentru a cuantifica, în timp real, propriile date (privind sănătatea sau bunăstarea) și pentru a le partaja – de regulă, prin intermediul rețelelor de socializare (în comunitatea virtuală, cu alte persoane care recurg la această metodă, cu medicul de familie ș.a.). Auto-măsurarea conectată este „practica de a utiliza obiecte conectate pentru a măsura variabile fiziologice legate de alimentația, activitatea fizică sau somnul unei persoane” (obiectele conectate pot fi un ceas, un pedomer sau un telefon mobil, care indică, de exemplu, numărul de calorii absorbite, numărul de pași /ritmul cardiac sau ochelari, ceasuri, ale căror funcții au fost extinse prin încorporarea unor senzori specifici informaticii vestimentare)³⁶.

Un element de particularitate este acela că utilizatorii dezvăluie în mod voluntar informații sensibile.

31. Datele sunt preluate după «Live smart, go digital: biometric identification in the „Smart City” concept», *op. cit.*

32. A se vedea, («Live smart, go digital: biometric identification in the „Smart City” concept», *op. cit.*

33. Informațiile sunt redată după Menjun Tao, Richard Jiang, Carolyn Downs, „Ethics of Face Recognition in Smart Cities Toward Trustworthy AI”, în *Big Data Privacy and Security in Smart Cities: Advanced Sciences and Technologies for Security Applications*, 23-52; Michael I. Stein, «A year later, progress continues on Cantrell program to ID „high-risk” residents, but few details available», *The Lens*, 2.06.2019, disponibil pe pagina <https://thelensnola.org/2019/06/03/a-year-later-progress-continues-on-cantrell-program-to-id-high-risk-residents-but-few-details-available/>; Ali Winston, „Palantir has secretly been using New Orleans to test its predictive policing technology”, *The Verge*, 27.02.2018, <https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd> (paginile au fost accesate la data de 20.06.2024).

34. A se vedea, Maximilien Lanna, „La protection des données à caractère personnel à l'épreuve de l'automesure connectée”, thèse, Université Paris II – Panthéon Assas, 2019, p. 15.

35. Definiția este oferită de Comisia informatică și libertății, care funcționează în Franța (CNIL) (<https://www.cnil.fr/fr/definition/quantified-self>, accesat la 20.06.2024).

36. JORF, Avis divers, *Commission d'enrichissement de la langue française*, n° 0054, 4 martie 2017, textul 92, disponibil pe pagina <https://www.legifrance.gouv.fr/jorf/jo/2017/03/04/0054>, accesat la data de 20.06.2024.



Ei nu doar că măsoară și înregistrează propriile informații, dar procedează și la partajarea acestora în locații specifice (*site-uri web*, rețele sociale). Cel mai probabil, operațiunea partajării (cu alți utilizatori) este unul dintre motivele care fidelizează. Sinele cuantificat este la confluența a două tendințe: pe de o parte, temerea dezvăluirii datelor personale către terți, iar, pe de altă parte, încredințarea voluntară a unui volum foarte mare de informații ce privesc aspectele intime ale personalității. Accesul la date este posibil pentru fabricantul dispozitivului și pentru terți. Senzorii, camerele, microfoanele încorporate înregistrează date pe care le pot transmite fabricantului. De asemenea, existența interfețelor de programare a aplicației pentru dispozitivele de informatică vestimentară permite, de asemenea, crearea de aplicații de către terți, care primesc acces la datele colectate de aceste obiecte. De exemplu, aplicația *Wear OS by Google* (fosta aplicație *Android Wear*) are rolul de a sincroniza *smartwatch*-ul și telefonul, pentru o utilizare cu eficiență sporită a ceasului. *Smartwatch* are funcții pentru monitorizarea calității somnului, contorizarea pașilor, monitorizarea tensiunii arteriale, alertă pentru sedentarism, monitorizarea activității de fitness, captură foto de la distanță, alertă apeluri și mesaje, calculator (aceste funcții se adaugă celor clasice – ceas, alarmă).

Unul dintre riscurile majore este **riscul creării de profiluri alimentate de datele personale**. S-a menționat, pe bună dreptate, că datele de geolocalizare privind călătoriile, locul de muncă, obiceiurile alimentare, activitatea sportivă, tiparele de somn reprezintă elemente pe care furnizorii de servicii de cuantificare personală pot elabora profiluri detaliate ale utilizatorilor. La acuratețea profilurilor contribuie interconexiunile ce pot fi realizate între seturile de date din surse diferite, precum și prelucrarea algoritmică (din ce în ce mai sofisticată) a acestor informații. Dezvoltarea pe scară largă a obiectelor conectate favorizează riscul informațional, înțeles ca pierdere a controlului individului asupra datelor personale³⁷.

V. Un numitor comun al riscurilor. *Big data* (*mégadonnées*)

Evoluțiile *Internet of things* vor devoala noi riscuri, astfel că un inventar complet ar fi hazardat. Universul obiectelor conectate nu este monocolor. *Internet of Things* înseamnă informatică și drept, cu tranzitarea inteligenței artificiale, eticii, sociologiei³⁸. Pentru *smart cities*, pare că „succesul” (privit „din afară”) constă în exploatarea inedită a resurselor. Totuși, la o privire atentă, nici industria, nici transportul local, nici tehnologiile avansate de protecție a mediului ș.a., nu sunt suficiente pentru a fi în prezența unui *smart city*. Aceste direcții sunt constante care descriu orașele inteligente – însă, punerea în valoare are loc prin intermediul prelucrării datelor cu caracter personal (în particular, prin valorificarea *big data*). Pe bună dreptate, s-a menționat că „Un oraș inteligent nu ar putea funcționa fără colectarea a mii de date (adesea anonime). Deoarece principiul orașelor inteligente este acela de a răspunde nevoilor precise ale cetățenilor, aceste proiecte necesită colectarea de date, dintre care unele pot fi descrise ca «date cu caracter personal». În majoritatea proiectelor «*smart cities*», putem vorbi chiar de *big data* în măsura în care avem de-a face cu mii de date, adesea anonimizate, care sunt agregate pentru a oferi un rezultat diferit de cel al datelor luate izolat. Prin agregarea a mii de date se pot obține rezultate și concluzii, care permit implementarea unor infrastructuri și servicii «inteligente», răspunzând nevoilor cetățenilor. Aceste date sunt, prin urmare, esențiale pentru succesul unui proiect «*smart cities*»: ele permit atât funcționarea serviciilor existente, cât și dezvoltarea de noi servicii care să răspundă nevoilor comunității³⁹. Din perspectiva drepturilor inerente ființei umane, remarcăm riscurile asociate prelucrării masive de date cu caracter personal. Nucleul universului obiectelor conectate este *big data*. Un sistem cu o arie imensă de obiecte interconectate este condiționat de prelucrarea și gestionarea unui volum foarte mare de date cu caracter personal. Mecanismul care fundamentează internetul obiectelor este conectarea dispozitivelor prin intermediul stocării, structurării, transferului de informații. Existența și succesul *Internet of Things* sunt strict dependente de operațiunile de prelucrare a datelor personale, doar astfel fiind posibile asigurarea

37. Maximilien Lanna, „La protection des données à caractère personnel à l'épreuve de l'automesure connectée”, *op. cit.*, p. 32, p. 36.

38. Una dintre cele mai dezbătute probleme are în vedere etica sau morala inteligenței artificiale (implicit, interogația vizează etica sau morala internetului obiectului). În paralel cu avantajele majore, în multe domenii, temerea știrbirii drepturilor și libertăților este justificată. Pentru o privire de ansamblu asupra dreptului, moralei, standardelor morale, a se vedea, Emanuel Tăvală, „Realizarea dreptului din perspectiva moralității sale”, *Acta Universitatis Lucian Blaga*, Seria Jurisprudentia, nr. 1 (2022), p. 38-49.

39. Thibault Verbiest, «Le „data”, moteur des projets „*smart cities*»», *Revue Lamy droit de l'immatériel*, nr. 140 (2017).

autonomiei captării de date, transferul informațiilor, comunicarea în rețea și interoperabilitatea⁴⁰. Cu aceste operațiuni, orașele inteligente ar putea colecta și utiliza o cantitate mare de date, dintre care unele sunt de natură sensibilă. În plus, orașele inteligente ar putea implica procesarea datelor cu ajutorul instrumentelor de analiză și algoritmilor. În consecință, comentatorii au exprimat preocupări legate de protecția vieții private, în sensul că, potențiala colectare de date despre rezidenți, precum și metodele de prelucrare a acestor informații, ar putea contribui la supravegherea guvernamentală⁴¹.

Obiectele de tip *quantified self* acumulează și dezvăluie cantități semnificative de informații cu privire la utilizator. De pildă, dispozitivele conectate din domeniul sănătății sunt un instrument al geolocalizării. Astfel, societatea Asthmapolis (S.U.A.) utilizează monitorizarea GPS pentru produsele destinate astmaticilor. Produselor comercializate li se atașează dispozitive *Bluetooth* de mici dimensiuni care se conectează la telefonul mobil. Cu ajutorul unei aplicații mobile se colectează date privind momentul și locul folosirii inhalatorului de către bolnavi. Utilizarea aplicației GPS a telefonului mobil conduce la identificarea cu exactitate a locației. Colectarea volumului mare de date permite identificarea numărului de crize de astm, a severității acestora, a condițiilor care favorizează sau determină crizele de astm, dar sprijină, totodată, profilaxia bolii⁴². Un alt exemplu: inocență la prima vedere, păstrarea evidenței numărului de pași nu se integrează (la prima vedere) datelor referitoare la sănătate. Relevanța datelor care privesc sănătatea apare însă dintr-o dublă perspectivă. Sunt informații care, de sine stătător, furnizează elemente din tabloul sănătății – de exemplu, datele privind tensiunea. Apoi, sunt date care, în corelație cu alte informații, pot oferi predicții cu privire la riscuri pentru sănătate – de pildă, informațiile privind tensiunea, greutatea și înălțimea persoanei pot fi relevante pentru riscul cardiovascular⁴³. Una dintre soluțiile care se află la îndemâna fabricanților obiectelor conectate și a furnizorilor este *privacy by design*. Ocrotirea vieții private nu este o chestiune ulterioară producerii și punerii în funcțiune a sistemelor de inteligență artificială. Asigurarea confidențialității și securității trebuie să fie implicită (*by design*) – în acest mod, riscurile și beneficiile sunt estimate începând cu momentul concepției. Regulamentul privind inteligența artificială face trimitere la reducerea la minimum a datelor, prin măsuri cum sunt: anonimizarea, criptarea, folosirea unei tehnologii care permite să se aplice algoritmi datelor și antrenarea sistemelor de inteligență artificială, fără ca aceste date să fie transmise între părți și fără ca datele primare sau datele structurate să fie copiate, fără a aduce atingere cerințelor privind governanța datelor prevăzute în prezentul regulament (considerentul 69). *Privacy by design* este o modalitate de natură tehnică (cu caracter preventiv), complementară cadrului reglementar al protecției vieții private.

Pentru a promova reducerea la minimum a datelor, produsele trebuie concepute astfel încât persoanelor vizate să li se ofere posibilitatea de a utiliza dispozitivele în mod anonim sau într-un mod cât mai puțin intruziv cu putință în ceea ce privește viața privată. De asemenea, deținătorii de date ar trebui să limiteze cât mai mult posibil ieșirea de date din dispozitiv (de exemplu, prin anonimizarea datelor)⁴⁴.

40. Cu privire la crearea unor algoritmi de filtrare pe care furnizorii de servicii online de partajare de conținut sunt obligați să îi instituie, pentru a nu le fi antrenată răspunderea, potrivit Legii nr. 8/1996 cu privire la dreptul de autor și a drepturilor conexe, a se vedea A. Circa, „Răspunderea furnizorilor de servicii digitale prin prisma dreptului de autor. Perspectiva jurisprudențială română”, *Acta Universitatis „Lucian Blaga”*, Seria Iurisprudentia, nr. 1 (2022), p. 25.

41. Orașul New York a lansat o aplicație care a facilitat rezidenților stocarea și prezentarea dosarului de vaccinare și informațiilor privind testarea COVID-19; orașul Kansas City (Missouri), a instalat senzori de calitate a aerului în zonele de transmitere ridicată a virusului, pentru a contribui la reducerea ratei de infectare și la îmbunătățirea calității aerului (acest proiect a făcut parte dintr-un program de granturi cu National Science Foundation și a fost extins la Cleveland, Ohio și Chattanooga, Tennessee). Informațiile au fost preluate după Linsey Tonsager, Jayne Ponder, „Privacy Frameworks for Smart Cities”, *Journal of Law and Mobility*, (2022): 1-13.

42. Pentru exemplificare, Aurelian Titirișcă, „Big data and the internet of things, Study case USA healthcare”, *Management Intercultural*, nr. 1 (2015): 214.

43. CNIL, Cahier IP2 - *Le corps, nouvel objet connecté*, 24 octobre 2017, *Du Quantified Self à la M-santé : les nouveaux territoires de la mise en données du monde*, p. 14, disponibil la adresa <https://linc.cnil.fr/cahier-ip2-le-corps-nouvel-objet-connecte>, consultat la data de 20.06.2024.

44. Soluția a fost avansată în raport cu o gamă largă de produse și servicii, inclusiv obiecte conectate, dispozitive medicale și asistenți virtuali. A se vedea, European Data Protection Board, *Avizul comun nr. 2/2022 al CEPD-AEPD privind Propunerea de regulament al Parlamentului European și al Consiliului privind normele armonizate pentru un acces echitabil la date și o utilizare corectă a acestora (Legea privind datele)*, adoptat la 4 mai 2022, p. 2, disponibil pe pagina https://www.edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-2022-proposal-european_ro, accesat la 20.05.2024.



VI. Concluzii

« – *Nous voulons vous implanter cette puce RFID dans le corps. – Oh non! Cela viole mes droits! – Nous voulons vous implanter cette puce RFID dans le corps et cela fait aussi portable, appareil photo numérique et baladeur MP3. – Oh, cool!*»⁴⁵. Conștientizarea riscurilor pentru drepturile și libertățile individuale nu va fi de natură a obstacula *Internet of Things*. Balanța va înclina spre asimilarea noilor achiziții în materie de noi tehnologii, iar tendința spre lumea „*smart*” se va accentua, grație prezenței coplesitoare a obiectelor cu funcțiuni de facilitare a cotidianului. Vom constata că suntem înconjurați de obiecte inteligente, a căror funcționare vulnerabilizează controlul asupra informațiilor cu caracter personal.

Bibliography

- Bruguière, Jean-Michel and Gleize, Bérengère. *Droit des personnes*. [Personal Law]. Paris: Lefebvre Dalloz, first edition, 2023.
- C.C. Hageanu. *Dreptul familiei* [Family Law], 3rd revised and added edition (Bucharest: Hamangiu, 2023).
- Circa, Adrian. “Răspunderea furnizorilor de servicii digitale prin prisma dreptului de autor. Perspectiva jurisprudențială română” [The Liability of Digital Service Providers Through the Lens of Copyright Law. The Romanian Jurisprudential Perspective]. *Acta Universitatis Lucian Blaga, Seria Iurisprudentia*, no. 1 (2022).
- CNIL. Cahier IP2 – Le corps, nouvel objet connecté, 24 octobre 2017, Du Quantified Self à la M-santé : les nouveaux territoires de la mise en données du monde [CNIL, Cahier IP2 – The body, the new connected object, 24 October 2017, From Quantified Self to M-health: the new territories of the data world]. <https://linc.cnil.fr/cahier-ip2-le-corps-nouvel-objet-connecte>.
- European Data Protection Board, Avizul comun nr. 2/2022 al CEPD-AEPD privind Propunerea de regulament al Parlamentului European și al Consiliului privind normele armonizate pentru un acces echitabil la date și o utilizare corectă a acestora (Legea privind datele), adoptat la 4 mai 2022 [European Data Protection Board, EDPS-EEPA Joint Opinion No 2/2022 on the Proposal for a Regulation of the European Parliament and of the Council on harmonized rules for fair access to and fair use of data (Data Act), adopted on 4 May 2022], https://www.edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-2022-proposal-european_ro
- Giffinger, Rudolf, Christian Fertner, Hans Kramar, Robert Kalasek, Natasa Pichler-Milanović, Evert Meijers, Smart cities – Ranking of European medium-sized cities, Final Report, Centre of Regional Science (SRF). Vienna University of Technology, 2007. 10–12.
- Gluckert Smith, Marianne. “Tracing Property Interests: How Mandatory COVID-19 Contact Tracing Conflicts with the Maryland Constitution and Trade Secret Law.” *University of Baltimore Law Forum*, no. 2 (2022): 202–203.
- Griffin, Greg P. and Jiao, Jungfeng. “Where Does Bicycling for Health Happen? Analyzing Volunteered Geographic Information Through Place and Plexus.” *Journal of Transport & Health*, no. 2 (2015): 238–247.
- Grupul de lucru „Articolul 29” pentru protecția datelor, Avizul nr. 8/2014 cu privire la evoluțiile recente din sfera internetului obiectelor, 1471/14/RO WP 223 [Article 29 Data Protection Working Party, Opinion No 8/2014 on Recent Developments in the Internet of Things, 1471/14/RO WP 223]. dataprotection.ro.
- Heesch, Kristiann C., Bruce James, Tracy L. Washington, Kelly Zunig, and Matthew Burke. “Evaluation of the Veloway: A natural experiment of new bicycle infrastructure in Brisbane, Australia.” *Journal of Transport & Health*, no. 3 (2016): 366–376.
- Hinsdale, Eric, and Clobridge, Abby. “The Dark Side of Open Data.” *Information Today*, november/december (2018). <https://www.infotoday.com/OnlineSearcher/Articles/The-Open-Road/The-Dark-Side-of-Open-Data-128477.shtml>
- Irinescu, Lucia. “Noi provocări în era digitală. Politica de concurență” [New Challenges in the Digital Era. Competition Policy]. *Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Științe Juridice LXV* (2019).
- Jesticoa, Ben, Trisalyn Nelsona, and Meghan Wintersb. “Mapping Ridership Using Crowdsourced Cycling Data.” *Journal of Transport Geography*, vol. 52 (2016): 90–97.
- Landau, Susan and Vargas Leon, Patricia. “Reversing Privacy Risks: Strict Limitations on the Use of Communications Metadata and Telemetry Information.” *Colorado Technology Law Journal*, no. 2 (2023).
- Lanna, Maximilien. “La protection des données à caractère personnel à l’épreuve de l’automatisme connecté” [Personal data protection put to the test by connected self-measurement], thesis, University Paris II – Panthéon Assas, 2019.
- Marcu, Lucian. “Întâmpinarea în procesul civil I. Conținutul întâmpinării și sancțiunile aplicabile în cazul nerespectării dispozițiilor legale în materie” [Defendant’s Response in the Civil Process (I). Content of the Response and Sanctions Applicable in the Case Non-Fulfillment of Legal Provisions]. *Acta Universitatis Lucian Blaga, Series Iurisprudentia*, no. 2 (2017).

45. Traducerea în franceză este preluată după Laure Marino, „Le big data bouscule le droit”, *Revue Lamy droit de l’immatériel*, nr. 99 (2013): 57: « – We want to implant this RFID tag in you. – That violates my rights! – We want to implant this RFID tag in you and it’s also a cellphone, digital camera, and MP3 player – Cool! » Image David Farley, 2006, en ligne sur <http://ibiblio.org/dave/drfun.html> (Laure Marino, *loc. cit.*).

- Marcu, Lucian. "Întâmpinarea în procesul civil II. Excepții de la regula obligativității întâmpinării" [Procedural Act of the Respondent in the Civil Process. II. Exceptions to the Rule of Compulsory Response from the Respondent]. *Acta Universitatis Lucian Blaga, Series Iurisprudentia*, no. 1 (2018): 102–114.
- Marino, Laure. "Le big data bouscule le droit" [Big Data Is Shaking Up the Law]. *Revue Lamy droit de l'immatériel*, no. 99 (2013).
- Normele de drept civil privind robotica. Rezoluția Parlamentului European din 16 februarie 2017 conținând recomandări adresate Comisiei referitoare la normele de drept civil privind robotica, publicate în JO C 252/239/18.07.2018 [Civil law rules on robotics. European Parliament resolution of February 16, 2017 with recommendations to the Commission on civil law rules on robotics, published in JO C 252/239/18.07.2018].
- Orga-Dumitriu, Gina. *Instituții de drept public și privat* [Public and private law institutions]. Bucharest: C.H. Beck, 2011.
- Orientări în materie de etică pentru o inteligență artificială (IA) fiabilă, Grupul de experți la nivel înalt privind inteligența artificială, document publicat în 8.04.2019 [Ethical Guidance for Reliable Artificial Intelligence (AI), High-Level Expert Group on Artificial Intelligence, published 8.04.2019], <https://op.europa.eu/ro/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>.
- Osei-Bonsu, William, Aviel Stein, Michael Boswell. "The Current Ethical and Regulatory Status of the Internet of Medical Thing (IoMT) and the Need of a New IoMT Law." *The Journal of Healthcare Ethics & Administration*, no. 2 (2018).
- Pérez-Peña, Richard, and Matthew Rosenberg. "Strava Fitness App Can Reveal Military Sites, Analysts Say." *The New York Times*, January 29, 2018. <https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html>.
- Rannou, Hervé. "L'Internet des objets: d'une vision globale à des applications bien plus éparses" [The Internet of Things: from a global vision to much more scattered applications]. *Annales des mines – réalités industrielles*, no. 2 (2013): 70–118.
- Rastogi, Rohit. "Using ECG Authentication for Biometrics in Smart Cities." *International Journal of Systems and Software Security and Protection*, no. 1 (2023).
- Stein, Michael I. "A year later, progress continues on Cantrell program to ID 'high-risk' residents, but few details available." *The Lens*, June 2, 2019. <https://thelensnola.org/2019/06/03/a-year-later-progress-continues-on-cantrell-program-to-id-high-risk-residents-but-few-details-available/>
- Sudre, Frédéric. *Drept european și internațional al drepturilor omului* [European and International Human Rights Law]. Iași: Polirom, 2006.
- Sun, Yeran and Mobasher, Amin. "Utilizing Crowdsourced Data for Studies of Cycling and Air Pollution Exposure: A Case Study Using Strava Data." *International Journal of Environmental Research and Public Health*, no. 3 (2017).
- Tanislav, Eliodor. "Ocrotirea penală a dreptului la intimitate" [Criminal protection of the right to privacy]. *Revista de drept penal*, no. 3 (1998).
- Tao, Menjun, Richard Jiang, Carolyn Downs. "Ethics of Face Recognition in Smart Cities Toward Trustworthy AI." *Big Data Privacy and Security in Smart Cities: Advanced Sciences and Technologies for Security Applications*, edited by Ruchard Jiang et al., 23–52 (Springer International Publishing, 2022).
- Tăvală, Emanuel. Realizarea dreptului din perspectiva moralității sale [The Concept of Realising the Law from the Perspective of Its Morality], *Acta Universitatis Lucian Blaga, Seria Iurisprudentia*, no. 1 (2022): 38–49.
- Titirișcă, Aurelian. "Big data and the internet of things, Study case USA healthcare." *Management Intercultural*, no. 1 (2015).
- Tonsager, Linsey, and Ponder, Jayne. "Privacy Frameworks for Smart Cities." *Journal of Law and Mobility* (2022): 1–13.
- Verbiest, Thibault. "Le 'data', moteur des projets 'smart cities'" [Data, the driving force behind "smart cities" projects]. *Revue Lamy droit de l'immatériel*, no. 140 (2017).
- Vocabulaire de l'intelligence artificielle (liste de termes, expressions et définitions adoptés), JORF n° 0285/9. Union Internationale des Télécommunications, Recommandation UIT-T Y.2060, Série Y: infrastructure mondiale de l'information, protocoles internet et réseau de prochaine generation – Cadre général et modèles architecturaux fonctionnels, 6/2012, 12.2018 [Vocabulary of artificial intelligence (list of adopted terms, expressions and definitions), JORF n° 0285/9. International Telecommunication Union, Recommendation ITU-T Y.2060, Series Y: Global Information Infrastructure, Internet Protocol and Next Generation Network – General Framework and Functional Architectural Models, 6/2012, 12.2018].
- Winston, Ali. "Palantir has secretly been using New Orleans to test its predictive policing technology." *The Verge*, February 27, 2018. <https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd>.