**ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI**
**TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II**

# INTERNETUL LUCRURILOR. PERSPECTIVA JURIDICĂ

# INTERNET OF THINGS. LEGAL PERSPECTIVE

**ANDA CRIȘU-CIOCÎNTĂ**[1]

**Rezumat:** Se pare că într-un viitor nu prea îndepărtat „Internetul lucrurilor", zis și "Internet of Things" (IoT), va deveni un mod de viață pentru mare parte a omenirii. Într-o redare succintă, Internetul lucrurilor presupune conectarea oricărui dispozitiv la Internet și/sau conectarea mai multor dispozitive între ele, cu scopul de a fi monitorizate și controlate de la distanță. Axarea producătorilor pe cercetări menite să descopere cele mai sofisticate modalități de exploatare a lucrurilor conectate la Internet, precum și goana lor după obținerea rapidă a unor profituri cât mai consistente, face ca nivelul de securitate a acestor lucruri să rămână în plan secund. Securitatea scăzută a lucrurilor conectate la Internet va facilita acțiunile celor rău intenționați și, în cele din urmă, va influența criminalitatea. În prezentul material ne-am propus să realizăm o scurtă introducere în ceea ce poartă denumirea de „Internetul lucrurilor", după care să prezentăm o serie de fapte prevăzute de legea penală a căror comitere ar putea fi facilitată de dispozitivele inteligente conectate la Internet și controlate printr-o conexiune la distanță.
**Cuvinte cheie:** Internetul lucrurilor, securitate, dispozitive inteligente, provocări, criminalitate

**Summary**: As it seems like in a forthcoming future, "The Internet of things" also called "Internet of Things" (IoT), will become a way of living for most of the people. In a nutshell, the Internet of things implies the connection of every device to the Internet and/or the connection of multiple devices among each other in order to be monitored and controlled from the distance. The fact that manufacturers focused on research with the purpose of discovering the most sophisticated modalities of exploiting thing connected to the Internet, as well as their rush to quickly obtain as much consistent profits as possible determines the level of security of these things to remain on a second plan. The low security of the things connected to the Internet will encourage the actions of those who are malicious and, finally, it will influence the criminality. In this paper, we propose to make a brief introduction of what stands

[1] Doctorand, Universitatea „Alexandru Ioan Cuza" din Iași, Facultatea de Drept.

for “The Internet of things”, and then to present a series of criminal law facts, which, once committed, could be relieved by intelligent devices connected to the Internet and controlled through a remote connection.

**Key words**: Internet of things, security, intelligent devices, challenges, criminality

## 1. Introducere

Internetul, una dintre cele mai importante tehnologii a ultimilor aproximativ 60 de ani, care a reușit să ne influențeze modul de viață, a fost creat de oameni pentru oameni. În timp, lucrurile au evoluat, iar cercetările în domeniu au dus Internetul la un alt nivel, unul care presupune conectarea nu doar a oamenilor, ci și a lucrurilor. Spre deosebire de primele lucruri care au fost conectate la Internet - calculatorul și telefonul mobil - în cazul cărora oamenii sunt cei care în ultimă instanță se conectează la Internet, lucrurile din Internet of Things (IOT este prescurtarea uzuală) sunt dispozitive care interacționează mai mult între ele și, mai puțin, cu oamenii.

Internetul lucrurilor este un concept ce presupune conectarea oricărui dispozitiv la Internet și/sau conectarea mai multor dispozitive între ele, cu scopul de a fi monitorizate și controlate de la distanță. Se pare că într-un viitor nu prea îndepărtat se va ajunge la un Internet al tuturor lucrurilor – Internet of Everything – care să conecteze tot mai multe dispozitive ce ne vor asista viața de zi cu zi. Un astfel de lucru este posibil prin implementarea de senzori și abilități de comunicare tuturor dispozitivelor ce ne înconjoară. Prin senzorii implementați, dispozitivele vor culege date din mediul înconjurător, se vor conecta între ele și astfel vor transfera datele obținute care, în cele din urmă, vor ajunge la utilizator, acesta având posibilitatea de a controla activitatea dispozitivelor conform propriilor decizii.

În ultima perioadă, Internetul lucrurilor este într-o continuă expansiune. În acest sens, în anul 2016 erau conectate 6,4 miliarde de dispozitive, iar media zilnică a dispozitivelor nou conectate la Internet este de 10 milioane. Se estimează că până în 2020 vor exista peste 26 de miliarde de dispozitive conectate. Regula pentru viitor este aceea că „orice lucru care poate fi conectat la Internet, va fi conectat”[2].

Este incontestabil faptul că Internetul lucrurilor ne poate schimba viața în sens pozitiv datorită numeroaselor avantaje pe care le aduce. Ne putem imagina cum ar fi ca ceasul să ne trezească dimineața la ora stabilită,

[2] https://alinvelea.wordpress.com/2016/12/12/ce-este-internetul-lucrurilor/.

apoi să anunțe televizorul să pornească pe canalul preferat, expresorul să pregătească cafeaua, toasterul să prăjească pâinea, mașina să fie pregătită în momentul în care ieșim din casă și să ne indice traseul optim pentru a ajunge în cel mai scurt timp la destinația dorită (serviciu/școală). Sau dacă imprimanta știe când se va termina hârtia ori tonerul și va face comandă automat. Toate aceste lucruri sunt aproape posibile și, în mod evident, ne pot ușura viața, lăsându-ne mai mult timp liber pe care să-l petrecem după bunul plac.

Realitatea este că posibilitățile și conexiunile pot fi practic nelimitate, la multe dintre ele nici nu ne putem gândi sau nu putem înțelege pe deplin impactul lor, în acest moment. Internetul lucrurilor este o temă de larg interes întrucât presupune o mulțime de posibilități și de avantaje dar, în același timp, și multe provocări și neajunsuri. Din această din urmă categorie, problema securității credem că este cea mai importantă. Focusați pe ideea de a scoate cât mai repede și la costuri cât mai reduse un produs nou pe piață, producătorii echipamentelor IoT, de cele mai multe ori, lasă în plan secund aspectele ce țin de securitate. Lipsa ori insuficiența măsurilor de securitate fac ca tot mai multe dispozitive inteligente (telefoane, televizoare, camere de supraveghere, etc) să fie implicate în atacuri cibernetice de amploare. Multe companii au analizat sistemele inteligente disponibile în acest moment pe piață și au ajuns la concluzia că securitatea acestora este complet nesatisfăcătoare[3].

Dintre numeroasele probleme ce pot apărea ca urmare a lipsei sau insuficientei securități a IoT, atenția noastră va fi îndreptată asupra modului în care noua tehnologie poate influența criminalitatea sau, altfel spus, modul în care dispozitivele inteligente conectate la Internet pot favoriza fenomenul infracțional.

## 2. Influența IoT asupra criminalității

Pe lângă numeroasele avantaje pe care Internetul lucrurilor le poate aduce pentru omenire, această tehnologie poate crea și dezavantaje, unul dintre ele fiind acela al favorizării comiterii de fapte prevăzute de legea penală de către persoane rău intenționate. După părerea noastră, Internetul lucrurilor va putea fi folosit de către infractori ca un instrument menit să le

[3] https://cybersecuritytrends.ro/internetul-lucrurilor-vis-frumos-sau-cosmar/.

ușureze și, în același timp, să le favorizeze comiterea de activități infracționale.

Dacă până nu demult, comiterea de fapte prevăzute de legea penală prin intermediul Internetului era limitată la o sferă relativ restrânsă de infracțiuni specifice (avem în vedere infracțiunile privind comerțul electronic și cele de fraude comise prin sisteme informatice), odată cu apariția Internetului lucrurilor aria faptelor penale ce pot fi comise prin folosirea Internetului va cunoaște o extindere în sensul că va putea cuprinde infracțiuni dintre cele mai diverse. Având în vedere paleta extrem de largă a lucrurilor care pot fi conectate la internet și apoi interconectate între ele – obiecte casnice (de exemplu, aparate de cafea, smart Tv-uri, cuptoare electrice, frigidere, mașini de spălat), aparate medicale, autovehicule, instalații de foraj de petrol, etc - valorilor sociale ce pot fi lezate prin fapte comise și cu ajutorul IoT este una largă și diversă, drepturile fundamentale ale persoanei și patrimoniul fiind, în opinia noastră, cele care pot fi cel mai frecvent afectate

În continuare vom prezenta o serie de cazuri care redau legătura strânsă dintre comiterea de fapte prevăzute de legea penală și Internetul lucrurilor, cazuri în care noua tehnologie este un factor ce facilitează comportamentele ilicite.

O primă situație pe care ne-o imaginăm are în prim plan o plită electrică ce are încorporat un computer, iar printr-o aplicație este conectată la telefonul mobil, putând astfel primi comenzi de la distanță. Asta presupune că deținătorul unui astfel de obiect, în timp ce se află la birou de exemplu, poate porni plita electrică pentru ca fiul său minor (aflat în locuință) să-și încălzească laptele. Ne putem imagina că o persoană rău intenționată, prin spargerea contului și/sau a parolei, are acces la comenzile acelei plite electrice și astfel o poate deschide în timp ce în locuința nu se găsește nici o persoană, provocând astfel un incendiu care, în cele din urmă, duce la distrugerea locuinței. În acest caz poate fi reținută infracțiunea de distrugere a unui bun imobil, prin incendiere; infracțiunea fiind comisă fără ca autorul să se fi aflat în preajma bunului distrus în momentul comiterii faptei și nici măcar în momentul imediat premergător. Bineînțeles, infracțiunea de distrugere se va afla în concurs cu o serie de infracțiuni informatice (de exemplu, acces neautorizat).

O altă situație ipotetică pornește de la un aparat medical care monitorizează o persoană bolnavă și care poate fi controlat de pe Internet. Să

presupunem că aparatul medical este programat să controleze administrarea dozelor de medicamente prescrise pacientului, iar o persoană rău intenționată reușește să se conecteze la respectivul aparat și astfel, cu intenția de a ucide sau doar de a vătăma integritatea corporală sau sănătatea pacientului, îl manipulează în așa fel încât să trimită fie o doză mult mai mică, fie una mult mai mare din medicamentul prescris. Doza insuficientă sau supradoza poate fi fatală pentru pacient sau îi produce doar o lezare a integrității corporale sau a sănătății, situație în care putem vorbi de comiterea unor infracțiuni contra vieții sau infracțiuni contra integrității corporale sau sănătății persoanei. Observăm astfel că prin intermediul lucrurilor conectate la Internet pot fi comise și infracțiuni dintre cele mai grave, cum ar fi infracțiunea de omor.

Un alt caz ipotetic este acela în care un frigider este conectat la Internet și programat ca atunci când stocul la anumite produse este aproape epuizat să comande automat on-line acele produse la furnizor având, totodată, atașată o soluție pentru plata contravalorii produselor comandate (card, cont, PayPal, etc). Ca o vulnerabilitate ce poate apărea într-o astfel de situație este faptul că un infractor poate redirecționa comanda în așa fel încât produsele comandate și plătite să ajungă la o altă adresă decât cea unde se găsește obiectul în cauză. Practic beneficiarul produselor achiziționate este o altă persoană decât cea care le-a comandat și le-a plătit. Într-o astfel de situație poate fi reținută comiterea unor infracțiuni din categoria celor de fraudă comise prin sisteme informatice și mijloace de plată electronice. În plus, credem că poate fi pusă în discuție și existența unei infracțiuni de înșelăciune deoarece s-a produs o inducere în eroare prin prezentarea ca adevărată a unei împrejurări mincinoase (adresa de livrare a produselor comandate și plătite), fiind cauzată o pagubă materială. De remarcat faptul că persoana indusă în eroare nu este aceeași cu persoana în patrimoniul căreia s-a produs paguba materială însă această împrejurare nu constituie un impediment în reținerea infracțiunii de înșelăciune.

O altă situație pe care ne-o putem imagina vizează dispozitivele care permit autentificarea după amprentă sau după retină. Ca orice alte date, datele privind autentificarea sunt stocate într-un fișier care, atunci când nu este bine securizat, poate fi spart de un haker care le fură. Să ne imaginăm că respectivele date – amprenta sau retina – sunt folosite la dispozitivul de închidere-deschidere a ușii de acces într-o locuință. Dacă cineva fură cheia de acces în locuință, soluția este schimbarea yalei însă, retina și amprenta nu

mai pot fi schimbate. Dacă o persoană a ales să deschidă ușa la casă cu ochiul sau amprenta pe un dispozitiv slab securizat și un haker fură acele date, e ca și cum ar avea cheia de la casă care poate fi folosită ulterior pentru pătrunderea fără drept în locuință, fiind astfel facilitată comiterea infracțiunilor de violare de domiciliu sau violarea sediului profesional. De această dată, conectarea lucrurilor la Internet (în speță, dispozitivul de deschidere a ușii de acces) este de natură să-l ajute pe infractor, facilitându-i pătrunderea în imobil. Totodată, noul mod de pătrundere în domiciliu/sediu profesional se îndepărtează de modurile clasice, tradiționale de violare de domiciliu/sediu profesional.

Tot așa ne putem imagina cazul ușilor de garaj ce sunt conectate la wireless pentru a fi deschise din mașină și care pot fi folosite de către infractori pentru a intra în casă fără să mai fie nevoiți să apeleze la metodele clasice (spargerea și escaladarea geamului, efractarea sistemului de închidere a ușii de acces) și fără a declanșa sistemul de alarmă. Și într-o astfel de situație acțiunea de pătrundere fără drept în imobil este mult ușurată pentru infractor ca urmare a conectării la Internet a ușilor de garaj. Este facilitată astfel comiterea infracțiunii de violare de domiciliu și, în ipoteza în care pătrunderea se face în scopul sustragerii de bunuri, și a infracțiunii de furt sau, eventual, a celei de tâlhărie.

Însă, de departe cea mai la îndemână infracțiune pe care un infractor ar putea să o comită beneficiind de avantajele pe care le aduce Internetul lucrurilor este infracțiunea de violare a vieții private (art. 226 Cod penal). Multe dintre dispozitivele inteligente au sau pot avea încorporată o cameră Web și/sau microfon prin intermediul cărora putem fi „spionați” atunci când ne aflăm în spațiul nostru privat. Hakerii pot utiliza webcam-ul și microfoanele încorporate într-un Smart TV, de exemplu, pentru a vedea și a auzi tot ceea ce se întâmplă în fața acelui dispozitiv. Evident că în situații de acest gen putem vorbi de atingerea adusă vieții private în mod nelegal prin captarea sau înregistrarea de imagini sau ascultarea cu mijloace tehnice a unei persoane aflată într-un spațiu privat. Practica ne dovedește că în situații de acest fel, conduita ilicită a infractorului nu se oprește la violarea vieții private, ci, de cele mai multe ori, atunci când imaginile/înregistrările sunt compromițătoare pentru persoana vătămată continuă cu săvârșirea unor fapte de șantaj (art. 207 Cod penal). Practic, după ce intră în posesia unor imagini sau înregistrări pretins sau real compromițătoare, infractorul amenință

persoana vătămată cu darea în vileag a imaginilor/înregistrărilor deținute cu scopul de a obține un folos patrimonial.

## 3. Concluzii

Viitorul va aparține din ce în ce mai mult Internetului lucrurilor care are potențialul să schimbe radical modul în care interacționăm cu tehnologia, între noi și în societate. Dincolo de beneficiile pe care le aduce această nouă tehnologie, considerăm că trebuie conștientizate și riscurile pe care ea le implică.

În opinia noastră, principala problemă a dispozitivelor inteligente este securitatea care de cele mai multe ori este neglijată de producători din dorința de a face cât mai mult profit și a scoate un produs cât mai ieftin pe piață.

După părerea noastră, adoptarea unui cadru legislativ adecvat care să îi oblige pe producătorii de echipamente IoT să instaleze pe aceste echipamente soluții de securitate performante pentru a nu mai fi preluate atât de ușor, ar reprezenta o soluție viabilă pentru rezolvarea, cel puțin parțială, a problemei securității lucrurilor conectate la Internet. De asemenea, o altă soluție ar fi aceea a securizării dispozitivelor inteligente cu ultimele versiuni de software.

Potrivit unui studiu realizat de dată relativ recentă de Pew Internet Project Research, din marea majoritate a experților în tehnologie și utilizatori de Internet care au răspuns, 83% au fost de acord cu ideea că Internet of Things, cu sisteme informatice integrate și portabile (și sistemele dinamice corespunzătoare) vot avea efecte benefice larg răspândite până în 2025 și doar 17% dintre respondenți au susținut că aceasta tehnologie va avea efecte negative. Observăm astfel că opinia majoritară este în favoarea dezvoltării, extinderii Internet of Things, ceea ce presupune asumarea riscurilor pe care această tehnologie le implică și, totodată, identificarea soluțiilor menite să le diminueze pe cât mai mult posibil.