EUROPEAN DATA PROTECTION SUPERVISOR

Avizul 4/2015

Către o nouă etică digitală

Date, demnitate și tehnologie

11 septembrie 2015

Autoritatea Europeană pentru Protecția Datelor (AEPD) este o instituție independentă a UE, care răspunde, în temeiul articolului 41 alineatul (2) din Regulamentul 45/2001 „În ceea ce privește prelucrarea datelor cu caracter personal… de respectarea de către instituțiile și organele comunitare a drepturilor și libertăților fundamentale ale persoanelor fizice, în special, a vieții private a acestora", și „…de consilierea instituțiilor și organelor comunitare și a persoanelor vizate asupra tuturor aspectelor privind prelucrarea de date cu caracter personal". A fost numit în luna decembrie 2014 împreună cu adjunctul Autorității cu condiția specifică de a fi mai constructiv și mai proactiv. AEPD a publicat în martie 2015 o strategie pe cinci ani în care arăta cum intenționează să implementeze această condiție și că urmează să fie răspunzătoare de acest lucru.

Prezentul aviz apare în urma avizului anterior al AEPD privitor la Regulamentul general privind protecția datelor, care își propunea să asiste principalele instituții ale UE să ajungă la consensul potrivit în legătură cu pachetul de reglementări aplicabile, orientate către viitor, ce susține drepturile și libertățile individului. Ca Avizul privind sănătatea mobilă de la începutul anului 2015, acesta abordează problema digitalizării protecției datelor - al treilea obiectiv al Strategiei AEPD - „adaptarea principiilor de protecția datelor existente pentru a se potrivi cu arena digitală globală", ținând cont și de planurile UE pentru Piața unică digitală. Este compatibil cu abordarea Grupului de lucru prevăzut la articolul 29 asupra aspectelor de protecția datelor în legătură cu folosirea de noi tehnologii, cum ar fi „internetul obiectelor", la care AEPD a contribuit ca membru deplin al grupului.

Dignity	Demnitate
Future-oriented rules and enforcement	Reglementări orientate către viitor și punere în aplicare
Accountable controllers	Operatori responsabili
Empowered individuals	Mai multe drepturi pentru persoanele fizice
Innovative privacy engineering	Inginerie inovatoare pentru protecția vieții private
Ethics	Etică

„Demnitatea umană este inviolabilă. Aceasta trebuie respectată și protejată."

Articolul 1, Carta Drepturilor Fundamentale a Uniunii Europene

Drepturile fundamentale la viață privată și la protecția datelor cu caracter personal au devenit mai importante decât oricând pentru protecția demnității umane. Ele sunt consfințite în Tratatele UE și în Carta Drepturilor Fundamentale a Uniunii Europene. Ele permit indivizilor să-și dezvolte propriile personalități, să ducă vieți independente, să inoveze și să-și exercite alte drepturi și libertăți. Principiile de protecție a datelor definite în Carta Uniunii Europene - necesitate, proporționalitate, echitate, minimizarea datelor, limitarea scopului, consimțământ și transparență - se aplică întregii prelucrări de date, atât culegerii datelor cât și folosirii acestora.

Tehnologia nu ar trebui să dicteze valori și drepturi, dar nici relația dintre acestea nu ar trebui redusă la o falsă dicotomie. Revoluția digitală promite beneficii pentru sănătate, mediu, dezvoltarea internațională și eficiența economică. Ținând cont de planurile UE referitoare la o piață unică digitală, tehnologia de tip cloud computing, „internetul obiectelor", "volumele mari de date și alte tehnologii sunt considerate esențiale pentru competitivitate și dezvoltare. Modelele comerciale exploatează noi capacități pentru colectarea în masă, transmiterea instantanee, combinarea și reutilizarea informațiilor cu caracter personal în scopuri neprevăzute și sunt justificate de politici de confidențialitate lungi și impenetrabile. Acest lucru supune principiile protecției datelor la noi presiuni, simțindu-se nevoia unei gândiri noi privind modul în care sunt aplicate.

În mediul digital din zilele noastre, respectarea legii nu este de ajuns; trebuie să ținem cont de dimensiunea etică a prelucrării datelor. Cadrul de reglementare al UE lasă deja loc pentru decizii și protecții flexibile, de la caz la caz, în manipularea informațiilor cu caracter personal. Reforma cadrului de reglementare va fi un mare pas înainte. Există însă probleme mai serioase în ceea ce privește impactul tendințelor din societatea antrenată de date asupra demnității, libertății individului și funcționării democrației.

Aceste probleme au implicații inginerești, filozofice, juridice și morale. Prezentul aviz scoate în evidență câteva tendințe tehnologice majore ce ar putea presupune o prelucrare inacceptabilă a informațiilor cu caracter personal sau ar putea interfera cu dreptul la viața privată. Acesta conturează un „ecosistem de protecție a volumelor mari de date" pe patru niveluri pentru a răspunde provocării digitale: un efort colectiv, sprijinit de considerente etice.

(1) O reglementare orientată către viitor a prelucrării datelor și a respectării drepturilor la viața privată și la protecția datelor.

(2) Operatori responsabili, care stabilesc prelucrarea informațiilor cu caracter personal.

(3) Inginerie și concepție a produselor și serviciilor de prelucrare a datelor care țin cont de viața privată.

(4) Mai multe drepturi pentru persoanele fizice.

Autoritatea Europeană pentru Protecția Datelor dorește să stimuleze o discuție deschisă și informată în interiorul și în exteriorul UE, care să implice societatea civilă, proiectanți, întreprinderi, profesori universitari, autorități publice și autorități de reglementare. Noul consiliu deontologic pentru protecția datelor din UE pe care îl vom înființa la AEPD va ajuta

la definirea unei noi etici digitale, permițând o mai bună conștientizare a beneficiilor tehnologiei pentru societate și economie în moduri ce consolidează drepturile și libertățile persoanelor fizice.

CUPRINS

1. Date pretutindeni: Tendințe, oportunități și provocări

Cantitățile tot mai mari de informații cu caracter personal sunt colectate și prelucrate în moduri tot mai opace și complexe. Odată cu pătrunderea progresivă a calculatoarelor în afaceri și administrațiile publice în anii 1980, s-a răspândit percepția conform căreia practicile guvernelor și corporațiilor puternice în prelucrarea datelor cu caracter personal reduceau persoanele fizice la statutul de simple persoane vizate, punând în pericol drepturile și libertățile fundamentale. Ceea ce diferențiază valul actual de informații integrate și tehnologia comunicațiilor este omniprezența și puterea sa.

Anul trecut s-a raportat faptul că pe planetă existau mai multe dispozitive conectate decât persoane[1]. Creșterea capacității procesoarelor[2], a spațiilor de stocare și a lărgimii de bandă de transmisie înseamnă că există tot mai puține constrângeri tehnice la prelucrarea informațiilor cu caracter personal. Se preconizează că „internetul obiectelor" și analitica volumelor mari de date vor converge cu sisteme de inteligență artificială, prelucrarea limbajului natural și cu sisteme biometrice pentru a permite aplicații cu capacitate de învățare automatizată pentru inteligență avansată. Guvernele și întreprinderile sunt capabile să treacă dincolo de „extragerea datelor" până la „extragerea realității", care pătrunde în experiențele, comunicarea și chiar gândurile de fiecare zi[3]. Pe măsură ce societatea se adaptează la cerințele pieței digitale, în prezent se depun eforturi reînnoite pentru a preda programare copiilor mici[4]. Valorificarea acestor tendințe într-un sector în care UE este un consumator principal, dar lent în furnizarea serviciilor reprezintă o temă recurentă în strategia pieței unice digitale a Comisiei[5].

Aceste tendințe și multe dintre conceptele folosite astăzi, în ciuda prevalenței lor, sunt vagi și se suprapun între ele. Pentru a ajuta la stimularea unei dezbateri, dorim să evidențiem tendințe specifice care, deși nu sunt în mod evident exhaustive în opinia noastră, ridică cele mai importante probleme etice și practice pentru aplicarea principiilor de protecție a datelor.

1.1 Volumele mari de date

Volumele mari de date[6] se referă la practica de a combina volume imense de informații provenite din diverse surse și de a le analiza, folosind adesea algoritmi de autoînvățare pentru informarea deciziilor. Aceste informații nu sunt întotdeauna personale: datele generate de senzori pentru monitorizarea fenomenelor naturale sau atmosferice precum starea vremii sau poluarea sau pentru monitorizarea unor aspecte tehnice ale proceselor de producție nu sunt legate de „o persoană fizică identificată sau identificabilă"[7]. Una din cele mai importante valori ale volumelor mari de date pentru întreprinderi și guverne derivă însă din monitorizarea comportamentului *uman*, la nivel colectiv și individual, și rezidă în potențialul său predictiv[8].

Unul din rezultate ar fi apariția unui model de venituri pentru întreprinderile din domeniul internetului care se sprijină pe activitatea de urmărire online pentru a optimiza valoarea economică a tranzacțiilor pentru furnizorii de servicii, nu numai în ceea ce privește publicitatea țintită, ci și referitor la condițiile și prețurile polițelor de asigurare, ale creditelor și ale altor relații contractuale. Pe piața competitivă de atragere a atenției utilizatorilor, majoritatea oamenilor nu sunt conștienți de amploarea acestei urmăriri[9]. Aceste volume mari de date ar trebui considerate cu caracter personal chiar dacă s-au folosit tehnici de asigurare a anonimatului: devine și mai ușor de dedus identitatea unei persoane prin combinarea așa-ziselor date „anonime" cu alte seturi de date, inclusiv informații aflate la dispoziția publicului, de exemplu în mediile sociale[10]. Când acele date sunt comercializate în special

peste hotare și între jurisdicții, responsabilitatea pentru prelucrarea informațiilor devine o nebuloasă, fiind dificil de stabilit sau de aplicat conform legii privind protecția datelor, în special în lipsa oricăror standarde internaționale.

1.2 „Internetul obiectelor”

Multe dispozitive conectate la internet sunt deja banale, precum telefoanele inteligente, tabletele și automatele bancare și de check-in la aeroport. Până în anul 2020, conectivitatea se previzionează că va deveni o caracteristică standard, cu 25 de miliarde de obiecte conectate (comparativ cu 4,8 miliarde în 2015) ce variază de la telemedicină până la autovehicule, de la contoare inteligente până la o gamă întreagă de dispozitive staționare și mobile pentru a permite crearea unor orașe inteligente[11].

Acești senzori vor furniza informații imediate și granulare pe care birourile statistice și studiile nu le pot obține astăzi, dar care nu sunt neapărat mai exacte și pot fi chiar înșelătoare[12]. Cifra estimativă de 1,8 miliarde de conexiuni între mașini auto până în anul 2022 ar putea reduce accidentele și poluarea, ar putea crește productivitatea și autonomia vârstnicilor și a persoanelor cu dizabilități[13]. „Articolele de purtat” precum hainele și ceasurile de mână vor prelucra informații cu caracter personal la fel ca alte dispozitive conectate. Ele vor fi capabile să detecteze cheaguri de sânge și să monitorizeze condiția fizică și vindecarea rănilor; țesăturile conectate ar putea proteja împotriva unor medii extreme, de exemplu în stingerea incendiilor. Aceste dispozitive vor încărca date cu caracter personal direct în spațiul de stocare în cloud, conectat la rețele sociale și vor putea eventual difuza în mod public, permițând identificarea utilizatorilor și urmărirea comportamentului și mișcărilor indivizilor și mulțimilor[14].

Modul în care sunt manipulate aceste informații ar putea afecta nu numai viața privată a utilizatorilor dispozitivelor, inclusiv atunci când sunt folosite la locul de muncă, ci și drepturile altor persoane care sunt observate și înregistrate prin intermediul dispozitivului. Deși există puțin dovezi pentru o discriminare efectivă, este clar că volumul imens de informații cu caracter personal colectate de „internetul obiectelor” este de mare interes ca mijloc de maximizare a veniturilor prin stabilirea unor prețuri mai personalizate în funcție de comportamentul urmărit, în special în sectorul asigurărilor de sănătate[15]. Vor fi puse în discuție și alte reguli specifice domeniului, de exemplu atunci când dispozitivele ce presupun prelucrarea de date legate de sănătate nu sunt clasificate tehnic ca dispozitive medicale și ies de sub incidența reglementării[16].

1.3 Informatica ambiantă

Informatica ambiantă sau invizibilă se referă la o tehnologie esențială ce stă la baza „internetului obiectelor”. Una dintre cele mai evidente aplicații ale sale o reprezintă „casele inteligente” și „birourile inteligente”, compuse din dispozitive cu o capacitate sofisticată integrată de prelucrare a informațiilor, care promit o mai mare eficiență energetică și persoane mai informate, capabile să își influențeze consumul de la distanță (deși ar depinde de independența locuitorului de proprietar sau de administratorul clădirii). Va trebui clarificat foarte bine cine este responsabil de scopul și mijloacele de prelucrare a datelor cu caracter personal implicate în aplicațiile de informatică ambiantă, nu numai pentru protejarea drepturilor fundamentale ale persoanelor, dar și pentru alocarea adecvată a răspunderii pentru a asigura respectarea cerințelor de securitate generale ale sistemului.

1.4 Tehnologia de tip cloud computing

Tehnologia de tip cloud computing este cunoscută ca tehnologie centrală care permite atât capacități avansate de analitică și extragere, colectare și analitică de volume mari de date, precum și torentul de date de la „internetul obiectelor”, folosit în prezent de circa o cincime dintre persoanele fizice și juridice din UE[17]. Aceasta permite concentrarea datelor din nenumăratele dispozitive ale „internetului obiectelor” și se bazează pe disponibilitatea și conectivitatea unor volume enorme de date în unități de stocare și prelucrare pe scară largă din întreaga lume[18]. Se estimează că o mai largă adoptare a tehnologiei de tip cloud computing[19] în sectorul privat și cel public ar putea adăuga în total 449 de miliarde de euro la PIB-ul UE28 (0,71% din PIB-ul total al UE).

Controlul asupra informațiilor cu caracter personal este adesea împărțit între client și furnizorul de servicii de tip cloud, iar răspunderea pentru obligațiile de protecție a datelor nu este întotdeauna clară. Acest lucru ar putea însemna că în practică se oferă o protecție insuficientă. Aceste obligații nu depind de **locația fizică de stocare a datelor**. **Mai mult decât atât**, deși aplicațiile economice sunt sprijinite numai de o tehnologie de bază, însăși infrastructura tehnologiei de tip cloud computing ar putea deveni o infrastructură critică și ar putea crește dezechilibrele la nivel de putere pe piață, 30% dintre întreprinderi susținând că întâmpină dificultăți în dezabonarea de la furnizori sau în schimbarea acestora[20].

1.5 Modele economice dependente de date cu caracter personal

Aceste tehnologii au permis noi modele economice care se bazează pe informații generate nu numai prin furnizarea de servicii, dar și din alte surse precum prezența în mediile sociale pentru evaluarea riscurilor și bonității și pentru maximizarea veniturilor. Un model economic proeminent în zilele noastre este reprezentat de platforme ce leagă vânzătorii și cumpărătorii și care permit partajarea și redistribuirea produselor, serviciilor, abilităților și activelor. Adesea denumită „economie bazată pe partajare”, „consum bazat pe colaborare” sau platforme economice online sau mobile între persoane fizice,[21] aceste platforme pot oferi eficiențe economice clasice, pot injecta competitivitate pe piețe și pot reduce deșeurile. Valoarea lor globală este estimată la de patru ori valoarea de la 26 până la 110 miliarde USD în anii următori[22]. Aceste modele economice bazate pe date generează deja venituri enorme în partajarea automobilelor și închirierile de locuințe, precum și în tehnologia financiară și împrumutul social. Studiile arată că consumatorii apreciază abordabilitatea și convenabilitatea lor aparent mai mare[23].

Moneda acestor platforme este de obicei reputația utilizatorului, comentariile celorlalți utilizatori și verificarea identității. Acest lucru ar putea fi văzut ca o îmbunătățire a transparenței și responsabilizării, dar nu neapărat în legătură cu furnizorul platformei în sine. Marii actori de pe aceste piețe au fost criticați că ar ascunde date legate de reputație chiar de utilizatorii individuali la care se referă informațiile respective. Există un risc uriaș ca persoanele fizice să fie excluse din servicii pe baza unor reputații bazate pe date inexacte pe care nu le pot ataca sau cere să fie șterse. Sprijinirea pe date provenite din mai multe surse aduce în discuție și principiul minimizării datelor din dreptul UE. Dimensiunea impactului viitor asupra indivizilor și societății al modelelor economice prezente și viitoare bazate pe tehnologie merită o reflecție atentă[24].

1.6 Dronele și vehiculele autonome

Dronele, sau aeronavele semi-autonome, servesc în prezent unor scopuri în principal militare, dar sunt folosite tot mai mult în scopuri de supraveghere, cartografiere, transport, logistică și

siguranță publică, cum ar fi stingerea incendiilor[25]. Fotografiile, materialele video și alte date cu caracter personal culese de drone pot fi date la schimb în rețelele de telecomunicații. Utilizarea acestora riscă un amestec grav în viața privată și un efect paralizant asupra libertății de exprimare. Se pune problema cum ar putea fi reglementate eficient proiectarea și utilizarea acestora astfel încât persoanele vizate să își poată exercita drepturile de a accesa datele capturate de aceste aparate.

La sol, vehiculele autonome sau automobilele fără șofer vor schimba felul în care este folosită sau organizată călătoria individuală și ar putea estompa diferența dintre transportul privat și cel public. Se estimează că vor fi 12 milioane de vehicule complet autonome și 18 milioane de vehicule parțial autonome până în anul 2035, Europa numărându-se printre primii care le vor adopta[26]. Algoritmii care direcționează automobilele vor guverna decizii care ar putea fi legate în mod direct de integritatea fizică și chiar de viața sau moartea persoanelor, de exemplu în alegerea programată în cazul unui impact inevitabil. La fel ca și nevoia evidentă de claritate în ceea ce privește persoana responsabilă și răspunzătoare de controlul datelor și securitatea datelor, aceste aplicații ridică o serie de întrebări etice.

1.7 Tendințe cu un impact posibil mai mare, pe termen mai lung

Bioprintarea 3D de elemente organice, ce folosește copii de celule ale pacienților și „pansamente bio" cu colagen (adică date sensibile conform dreptului UE) pentru a crea șiruri succesive de celule vii, este estimată să devină în curând ușor disponibilă[27]. Acest lucru ar ușura furnizarea de părți anatomice umane personalizate și ar fi deosebit de valoros în zone mai sărace și post-conflict din lume. Bioprintarea ridică întrebări evidente pentru etica medicală, protejarea proprietății intelectuale și protecția consumatorului, însă, în același timp, deoarece se bazează pe prelucrarea de date intime și sensibile legate de sănătatea persoanelor, și pentru aplicarea regulilor de protecție a datelor.

Inteligența artificială, precum robotica, se referă la o cerință tehnologică pentru mașinile autonome, atât cele staționare, cât și cele mobile. Înaintarea sa va oferi un imens potențial dincolo de aplicarea sa curentă. Calculatoarele cu învățare profundă învață singure sarcini prin prelucrarea unor seturi de date extinse folosind (printre altele) rețele neurale care par să emuleze creierul. Cercetătorii și întreprinderile își propun să îmbunătățească învățarea nesupravegheată. Deja algoritmii pot înțelege și traduce limbile, pot recunoaște imaginile, pot scrie articole de știri și pot analiza date medicale[28]. Mediile sociale oferă cantități enorme de informații cu caracter personal, pre-etichetate eficient chiar de către persoanele fizice respective. Aceasta ar putea fi ultima dintr-o serie de îmbunătățiri cognitive pentru a crește capacitatea creierului uman, precum hârtia sau abacul sau integrate în aparate autonome, roboți, însă acum este momentul să luăm în considerare ramificațiile mai vaste pentru persoanele fizice și societate[29].

2. Un ecosistem pentru protecția volumelor mari de date

UE are acum ocazia de a deschide calea către demonstrarea modului în care guvernele, autoritățile de reglementare, operatorii, proiectanții, dezvoltatorii și persoanele fizice pot acționa mai bine împreună pentru a consolida drepturile și pentru a dirija, în loc să blocheze, inovația tehnologică. După spusele unui comentator, tendințele descrise în secțiunea a doua au „mărit golul dintre ceea ce este posibil și ceea ce este permis din punct de vedere legal"[30]. Contrar anumitor afirmații, protecția vieții private și a datelor reprezintă o platformă pentru un mediu digital sustenabil și dinamic, nu un obstacol. Autoritățile independente de protecție a datelor, cum este AEPD, au un rol esențial în risipirea acestor mituri și în a răspunde la

îngrijorările reale ale persoanelor fizice legate de pierderea controlului asupra informațiilor lor cu caracter personal[31].

Următoarea generație de date cu caracter personal probabil că va fi chiar mai puțin accesibilă persoanelor fizică la care se referă. Responsabilitatea pentru modelarea unei piețe unice digitale sustenabile este în mod necesar dispersată, însă este în același timp interdependentă, ca un ecosistem, având nevoie de o interacțiune eficientă între dezvoltatori, întreprinderi și autoritățile de reglementare în interesul persoanei fizice. În această secțiune prezentăm contribuția pe care o pot aduce acești patru actori esențiali.

2.1 Reglementare orientată spre viitor

Recent am solicitat UE să profite de această ocazie istorică de a institui reguli mai simple pentru manipularea informațiilor cu caracter personal care vor rămâne relevante pentru o generație[32]. Negocierile privind Regulamentul general privind protecția datelor și directiva pentru protecția datelor în sectoarele poliției și justiției se află în stadiile finale și în curând atenția va fi îndreptată către viitorul Directivei privind confidențialitatea în mediul electronic în ceea ce privește comunicările electronice și noul Regulament de reglementare a modului în care instituțiile și organismele UE în sine prelucrează datele cu caracter personal. Cu costul economic al colectării și stocării datelor aproape neglijabil, autorităților de protecție a datelor le va reveni obligația de a pune în aplicare cu consecvență aceste reguli pentru a evita „pericolul moral" al prelucrării excesive a datelor[33].

Strategia Pieței Unice Digitale recunoaște legătura dintre controlul unor volume mari de date și puterea pe piață. Aceasta împărtășește convingerea, exprimată în Avizul nostru preliminar din anul 2014 privind „Confidențialitatea și competitivitatea în era volumelor mari de date", că este nevoie de mai multă coerență în rândul autorităților de reglementare. UE deține deja instrumentele necesare pentru a redresa dezechilibrele de putere de pe piața digitală: de exemplu, procedurile antitrust în curs de desfășurare ale Comisiei Europene reprezintă o confirmare a predominanței dispozitivelor mobile pentru accesarea Internetului. În cadrul juridic existent este posibilă o aplicare mai holistică, cum ar fi printr-un oficiu de cliring UE pentru ca autoritățile de supraveghere să analizeze dacă situațiile individuale pot ridica probleme de respectare a regulilor de concurență și de protecție a consumatorului și a datelor. De exemplu:

- Solicitarea unei mai mari transparențe a prețului - numerar sau altfel - pentru un serviciu poate informa și facilita analiza cazurilor de concurență[34], și
- Detectarea unei discriminări inechitabile prin prețuri pe baza unei slabe calități a datelor și a unor profilări și corelări inechitabile[35].

Un dialog mai strâns între autoritățile de reglementare din diferite sectoare ar putea duce la un răspuns la solicitările tot mai mari de parteneriate globale ce pot crea un „fond comun" de date deschise în care datele și ideile, cum ar fi statisticile și hărțile, să poată curge și să fie disponibile și supuse schimburilor în interesul public, cu un risc mai mic de supraveghere, pentru a le oferi persoanelor fizice mai multă influență asupra deciziilor ce le afectează[36].

2.2 Operatori responsabili

Răspunderea presupune instituirea unor politici interne și a unor sisteme de control care asigură respectarea și furnizează dovezi pertinente în special autorităților de supraveghere independente.

Am adus argumente pentru eliminarea birocrației în legea privind protecția datelor, reducând la minim cerințele legate de documentația nenecesară pentru a crește la maxim spațiul oferit pentru o inițiativă mai responsabilă din partea întreprinderilor, susținută de îndrumări din partea autorităților de protecție a datelor. Principiul că datele cu caracter personal ar trebui prelucrate numai în moduri compatibile cu scopul/scopurile specifice în care au fost colectate este esențial pentru respectarea așteptărilor legitime ale persoanelor fizice. De exemplu, codurile de conduită, auditurile, certificarea, auditurile și o nouă generație de clauze contractuale și reguli corporative angajante pot ajuta la construirea unui trust robust pe piața digitală. Persoanele responsabile cu manipularea informațiilor personale ar trebui să fie mult mai dinamice și mai proactive și să părăsească așa-zisa tendință „Black Box" de discreție și opacitate a practicilor comerciale, solicitând în același timp o transparență și mai mare din partea clienților[37].

2.3 Ingineria sensibilă la viața privată

Inovațiile umane au fost dintotdeauna produsul activităților unor grupuri sociale speciale și al unor contexte specifice, reflectând de obicei normele sociale ale timpului respectiv[38]. Totuși, deciziile legate de proiectarea tehnologică nu ar trebui să dicteze interacțiunile noastre sociale și structura comunităților noastre, ci mai degrabă ar trebui să ne sprijine valorile și drepturile fundamentale.

UE ar trebui să dezvolte și să promoveze tehnici și metodologii inginerești care permit implementarea unor tehnologii de prelucrare a datelor care să respecte pe deplin demnitatea și drepturile persoanelor. Inginerii de sisteme și de programe software trebuie să înțeleagă și să aplice mai bine principiile confidențialității prin concepție în noi produse și servicii în cadrul fazelor de proiectare și al tehnologiilor. Responsabilitatea trebuie să fie susținută de o mai mare cercetare și dezvoltare a metodelor și instrumentelor pentru asigurarea unor audituri exacte și pentru stabilirea conformității operatorilor și persoanelor împuternicite de aceștia cu regulile, cum ar fi „etichetarea" fiecărei unități de date cu caracter personal cu „metadate" ce descriu cerințe de protecție a datelor.

Soluțiile inginerești ar trebui să le dea posibilitatea persoanelor care doresc să își păstreze confidențialitatea și libertatea prin anonimitate să facă acest lucru. UE ar trebui să promoveze conceperea și implementarea de algoritmi care ascund identitățile și strâng date pentru a proteja persoanele, punând în același timp în valoare puterea predictivă a datelor[39].

Astăzi trebuie să punem bazele pentru o abordare a acestor sarcini prin aducerea laolaltă a unor dezvoltatori și experți în protecția datelor din diferite zone în rețele extinse, cum ar fi Rețeaua Tehnică de Confidențialitate pe Internet (IPEN), care să contribuie la un schimb interdisciplinar fructuos de idei și abordări.

2.4 Mai multe drepturi pentru persoanele fizice

Un mediu „prosumator"

Persoanele fizice nu sunt simple obiecte pasive care solicită protecția legii împotriva exploatării. Tendințele digitale descrise mai sus prezintă oportunități pozitive pentru întărirea rolului persoanelor fizice. De exemplu, acum oamenii produc și consumă conținut și servicii și pot fi considerați tot mai mult responsabili în solidar cu furnizorii de servicii pentru prelucrarea datelor cu caracter personal, cu excepția cazului în care aceasta se face în scopuri pur „gospodărești"[40] (a apărut conceptul de „prosumatori" pentru a descrie această evoluție[41]). Între timp, monedele virtuale le oferă anonimitate utilizatorilor și evitarea

verificării tranzacțiilor de către terțe părți, prin urmare și costuri de tranzacționare mai mici pentru bunuri și servicii peste hotare. Pe de altă parte, anonimatul și natura inter-jurisdicțională (sau, am putea spune, *a-jurisdicțională*) a acestor monede virtuale lasă persoanele fizice să fie vulnerabile la fraudă și la piețe ilicite care sunt greu de detectat și investigat. Pe lângă obligațiile autorităților de reglementare, ale întreprinderilor și inginerilor, și cetățenii au o responsabilitate, și anume aceea de a fi conștienți, în alertă, critici și informați atunci când fac alegeri atât online, dar și offline[42].

Consimțământul

Mai mult decât atât, contrar gândirii tradiționale, nu întregul comportament uman poate fi explicat prin principii economice care presupun că ființele umane sunt pe deplin raționale și sensibile la stimulente economice[43]. Acesta este relevant pentru rolul viitor al consimțământului persoanei fizice pentru prelucrarea informațiilor cu caracter personal despre aceasta. Conform dreptului UE, consimțământul nu este singura bază legitimă pentru cele mai multe prelucrări. Chiar și atunci când consimțământul joacă un rol important, acesta nu îi scutește pe operatori de responsabilitatea pe care o au pentru ceea ce fac cu datele, în special atunci când a fost obținut un consimțământ generalizat pentru prelucrare pentru o gamă largă de scopuri.

„Proprietatea" asupra controlului și datelor

Persoanele fizice trebuie să fie capabile să conteste greșelile și distorsiunile inechitabile apărute de pe urma logicii folosite de algoritmi pentru a determina ipoteze și predicții. Ca exemplu, în SUA un studiu de aproape 3 000 de rapoarte de credit aparținând unui număr de 1 000 de consumatori a constatat că 26 la sută conțineau erori „semnificative" și probleme suficient de grave pentru a afecta punctajele de credit ale consumatorilor și, prin urmare, costul obținerii creditului[44].

Datele sunt adesea considerate o resursă, ca petrolul, ce poate fi comercializată, în mod ideal de către părți la fel de bine informate în legătură cu tranzacția[45]. Clienții nu sunt recompensați echitabil pentru informațiile lor personale ce sunt comercializate, iar unii au adus argumente în favoarea unui model de proprietate asupra datelor. Totuși, un control absolut asupra datelor personale este dificil de garantat - vor exista alte preocupări, cum ar fi interesul public și drepturile și libertățile celorlalți. Controlul este necesar, dar nu este suficient[46]. Totuși, demnitatea umană rămâne mereu o constantă, iar conform dreptului UE analogia proprietății nu poate fi aplicată ca atare informațiilor cu caracter personal, care au o legătură intrinsecă cu personalitățile individuale. În legea UE privind protecția datelor nu există nicio prevedere ca o persoană fizică să renunțe la acest drept fundamental.

O metodă alternativă prin care persoanele fizice ar putea să capete un mai bun control asupra datelor lor, aflând cine le accesează și în ce scop, ar putea fi utilizarea magazinelor de date personale sau a „seifurilor de date"[47]. Conceptul unui astfel de „magazin personal" are nevoie de mecanisme de securitate care să garanteze că numai entitățile autorizate de subiectul datelor pot accesa datele și numai acele porțiuni pentru care sunt autorizate. Magazinele de date cu caracter personal ar fi foarte eficiente în ceea ce privește informațiile actuale și cele constant actualizate, cum sunt datele geospațiale sau semnele de viață. Dincolo de protecțiile tehnice, utilizatorii de date ar fi obligați să respecte regulile referitoare la partajarea și utilizarea datelor. Concurența și posibilitatea de a schimba serviciul pe care îl folosește este singura putere foarte eficientă a unui consumator de a influența piața serviciilor aflate la dispoziția sa. Asigurarea portabilității conexiunilor, inclusiv a identificatorilor și a

informațiilor de contact, s-a dovedit a fi un factor puternic de concurență și a redus eficient prețurile la consumator în momentul în care piața telecomunicațiilor a fost liberalizată. Portabilitatea datelor, adică posibilitatea faptică și practică de a transfera majoritatea datelor proprii ale cuiva de la un furnizor de servicii la altul, este un punct de plecare eficient către asigurarea condițiilor necesare pentru o adevărată alegere a consumatorului.

3. Demnitatea în centrul unei noi etici digitale

Un cadru etic are nevoie să susțină blocurile structurale ale acestui ecosistem digital. AEPD consideră că un mai mare respect pentru demnitatea umană și apărarea acesteia ar putea fi contragreutatea la supravegherea pătrunzătoare și asimetria de putere cu care se confruntă în prezent persoanele fizice. Aceasta ar trebui să fie în centrul unei noi etici digitale.

3.1 Demnitatea și datele

În urma revoluției industriale din secolele al XVIII-lea și al XIX-lea, mișcarea drepturilor omului a căutat să asigure binele social mai larg prin reducerea obstacolelor în calea respectului pentru persoane. Acum UE și-a stabilit ca punct de plecare, prin Carta drepturilor fundamentale, și ca urmare a Declarației universale a drepturilor omului și a Convenției drepturilor omului, inviolabilitatea demnității umane. Demnitatea persoanei umane nu este numai un drept fundamental în sine, ci și o fundație pentru libertățile și drepturile ulterioare, inclusiv drepturile la viață privată și la protecția datelor cu caracter personal[48]. Încălcarea demnității poate include obiectificarea, caz în care o persoană este tratată ca un instrument ce servește scopurilor altcuiva[49]. Viața privată reprezintă o parte integrantă a demnității umane, iar dreptul la protecția datelor a fost conceput inițial în anii 1970 și 1980 ca o modalitate de a compensa potențialul de eroziune al confidențialității și demnității prin prelucrarea datelor cu caracter personal pe scară largă. În Germania, dreptul la „autodeterminare informațională” s-a bazat pe drepturile la demnitate personală și la libera dezvoltare a personalității stipulate la articolele 1 și 2 din Constituția Germaniei[50].

Totuși, în prima parte a secolului al XXI-lea, persoanelor fizice li se cere tot mai mult să-și dezvăluie mult mai multe informații cu caracter personal pe internet pentru a participa la activitățile sociale, administrative și comerciale, cu posibilitatea tot mai puțin limitată de a refuza acest lucru. Cu toată activitatea care există probabil în orice moment online, noțiunea de consimțământ liber și informat este plasată sub o tensiune enormă. „Firimiturile digitale” sunt aruncate în fiecare minut și combinate pentru a clasifica persoanele în timp real și pentru a crea profiluri multiple și uneori contradictorii. Aceste profiluri pot fi circulate în microsecunde fără cunoștința persoanelor în cauză și pot fi folosite ca bază pentru deciziile importante care le afectează.

Profilurile folosite pentru a prezice comportamentul oamenilor riscă stigmatizarea, consolidând stereotipurile existente, segregarea și excluderea socială și culturală[51], această „inteligență colectivă” subminând alegerea individuală și egalitatea de șanse. Aceste „bule filtrante” sau „camere de ecou personal” ar putea sfârși prin a înăbuși chiar creativitatea, inovația și libertatea de exprimare și asociere care au permis înflorirea tehnologiilor digitale.

Între timp, se folosește o stare continuă de excepție din motive de „securitate” pentru a justifica stratificarea multiplă a tehnicilor intruzive pentru monitorizarea activității persoanelor[52]. Pentru a înțelege acest „angrenaj de supraveghere” este nevoie de o perspectivă pe termen mai lung asupra efectelor generale asupra societății și comportamentului.

Împreună cu țările terțe, UE trebuie să caute cu atenție modul în care se poate garanta că aceste valori nu sunt respectate numai pe hârtie, fiind de fapt neutralizate în spațiul cibernetic. UE în mod special are acum o „fereastră critică" înainte de adoptarea în masă a acestor tehnologii pentru a construi valorile în structurile digitale ce ne vor defini societatea[53]. Acest lucru necesită o nouă evaluare dacă eventualele beneficii ale noilor tehnologii chiar depind de colectarea și analiza informațiilor identificabile personal a miliarde de persoane fizice. O astfel de evaluare ar putea chema dezvoltatorii să proiecteze produse care depersonalizează în timp real volume imense de informații neorganizate, făcând mai dificilă sau imposibilă distingerea unei anumite persoane fizice.

Recunoaștem deja că prelucrarea anumitor date, de exemplu a datelor genetice, nu trebuie numai să fie reglementată, ci și să fie supusă evaluării unor preocupări sociale mai largi de către comitetele de etică, de exemplu. Prin însăși natura lor, datele genetice nu se referă numai la o singură persoană, ci și la ascendenții și descendenții acesteia. Datele genetice nu servesc numai la identificarea relațiilor de familie. Elementele găsite în genele unei persoane pot furniza informații și despre părinții și copiii acesteia și pot duce la decizii ale operatorilor care le influențează șansele în viață încă dinainte de nașterea lor. Posibila concentrare de date cu caracter personal genetice în mâinile câtorva actori-gigant de pe piață are implicații pentru economiile de piață, precum și pentru persoanele vizate. O dependență tot mai mare de un sistem global de colectare și analiză a unui flux constant de date ar putea face societatea și economia mai vulnerabile la breșe de securitate și atacuri malițioase fără precedent.

Cadrul existent ar putea eșua dacă nu abordăm viitorul cu o gândire inovatoare. Există o cerere și o nevoie tot mai mare de a considera subiectul datelor ca o persoană, nu pur și simplu ca un consumator sau utilizator. Autoritățile de protecție a datelor cu adevărat independente au un rol crucial în împiedicarea unui viitor în care persoanele fizice sunt determinate de niște algoritmi și de variațiile continue ale acestora. Acestea trebuie să fie echipate pentru a exercita o „obligație de prudență" asupra persoanelor fizice și demnității lor online. Conceptele și principiile tradiționale în materie de viață intimă și protecție a datelor conțineau deja nuanțe etice pentru protecția demnității, cum ar fi locurile de muncă și sănătatea. Însă tendințele din ziua de astăzi au deschis un capitol cu totul nou și există o nevoie de a analiza dacă principiile sunt suficient de robuste pentru era digitală[54]. Însăși noțiunea de date cu caracter personal se va schimba probabil radical pe măsură ce tehnologia permite tot mai mult persoanelor fizice să fie reidentificate pe baza unor date presupuse ca fiind anonime. În plus, învățarea automatizată și contopirea inteligenței umane cu cea artificială vor submina conceptele de drepturi individuale și responsabilitate.

3.2 Un Comitet consultativ european pentru etică

Scopul nu este să descriem o imagine alarmantă a unei distopii. Discuțiile se află deja în derulare în sferele juridice, politice, economice, sociale, științifice și chiar religioase[55]. Abordările simpliste ce acordă avantaje unilaterale profitului economic sau supravegherii pentru securitate sunt probabil la fel de puțin utile ca și aplicarea supra-restrictivă a legilor existente care înăbușă inovația și progresul. Prin urmare, AEPD propune o analiză detaliată, extinsă și multidisciplinară pentru a oferi recomandări și a informa dezbaterea socială despre modul în care o societate liberă, democratică ar trebui să facă față provocărilor tehnologice.

Strategia AEPD[56] s-a concentrat pe dezvoltarea unei abordări etice a protecției datelor în care se recunoștea faptul că „fezabil, util sau profitabil nu este același lucru cu sustenabil" și care punea accentul pe „responsabilizarea față de respectarea mecanică a literei legii". Intenționăm să ajungem dincolo de comunitatea oficialilor, avocaților și specialiștilor IT ai UE până la

persoane eminente capabile să judece implicațiile pe termen mediu și lung ale schimbării tehnologice și ale reacțiilor în materie de reglementare. În lunile următoare, vom înființa la instituția noastră independentă un grup consultativ extern privind dimensiunea etică a protecției datelor pentru a explora relațiile dintre drepturile omului, tehnologie, piețe și modele economice în secolul al XXI-lea.

Comitetul nostru consultativ pentru etică va fi format dintr-un grup de elită constând din persoane distinse din domeniile eticii și filozofiei, sociologiei, psihologiei, tehnologiei și economiei, susținuți în funcție de necesități de experți suplimentari ce dețin cunoștințe și expertiză în domenii precum sănătatea, transportul și energia, interacțiunea socială și mediile de comunicare în masă, economia și finanțele, guvernanța și democrația, securitatea și poliția. Aceștia vor fi invitați să analizeze implicațiile etice mai largi ale modului în care sunt concepute datele personale și utilizate, acordând o transparență maximă deliberărilor acestora.

4. Concluzie: Este momentul să aprofundăm discuția

Confidențialitatea și protecția datelor sunt o parte a soluției, nu problema. Deocamdată, tehnologia este controlată de oameni. Nu este ușor de clasificat categoric aceste posibile evoluții ca fiind bune sau rele, de dorit sau de evitat, avantajoase sau dăunătoare, acest lucru fiind chiar mai dificil atunci când trebuie observate în context o serie de posibile tendințe. Factorii de decizie, dezvoltatorii de tehnologii, dezvoltatorii economici și noi toți trebuie să ne gândim serios dacă și cum dorim să influențăm dezvoltarea tehnologiei și aplicarea ei. Însă la fel de important este faptul că UE ia în considerare de urgență etica și locul demnității umane în tehnologiile viitorului.

Principiile de protecție a datelor s-au dovedit capabile să apere indivizii și viața lor privată împotriva riscurilor unei prelucrări iresponsabile a datelor. S-ar putea însă ca tendințele de astăzi să necesite o abordare complet nouă. Drept pentru care deschidem o nouă dezbatere: în ce măsură este suficientă aplicarea principiului echității și al legitimității? Comunitatea de protecție a datelor poate juca un nou rol folosind instrumente existente, cum ar fi verificările și autorizările prealabile - deoarece niciun alt organism nu este potrivit să examineze o astfel de prelucrare a datelor. Având în vedere dezvoltarea cu o viteză ametitoare a tehnologiei, inovației globale și corectitudinii umane, avem ocazia de a atrage atenția, de a suscita interesul și de a ajunge la un consens.

Cu prezentul aviz sperăm să oferim un cadru pentru o discuție mai largă și mai amănunțită despre cum poate UE să asigure integritatea valorilor sale în timp ce acceptă beneficiile noilor tehnologii.

Adoptat la Bruxelles, 11 septembrie 2015

(semnătura)

Giovanni BUTTARELLI
Autoritatea Europeană pentru Protecția Datelor

Note

[1] Sursa: GSMA Intelligence.

[2] „Legea lui Moore" conform căreia numărul de tranzistoare care pot fi amplasate pe un microcip se dublează la fiecare circa 18 luni s-a dovedit în general exactă; Moore, Gordon E. (19.4.1965). „Cramming more components onto integrated circuits", Electronics. 22.8.2011.

[3] Nathan Eagle, Alex (Sandy) Pentland, „Reality mining: sensing complex social systems", Journal Personal and Ubiquitous Computing Volumul 10 Ediția a 4-a, martie 2006, p. 255–268. Shoshana Zuboff în „Big Other: surveillance capitalism and the prospects of an information civilization", Journal of Information Technology (2015) 30, p. 75-89, scrie „Ca urmare a răspândirii medierii asistate de calculator, aproape fiecare aspect al lunii este redat într-o nouă dimensiune simbolică pe măsură ce evenimentele, obiectele, procesele și persoanele devin vizibile, cognoscibile și partajabile într-un mod nou". Zuboff preconizează o „creștere a unei noi arhitecturi universale" pe care o numește „Big Other", „un regim de instituții aflate în aceeași rețea, răspândit peste tot, care înregistrează, modifică și transformă în mărfuri experiențele de fiecare zi, de la prăjitoare de pâine până la corpuri, de la comunicare până la gânduri, toate în vederea stabilirii unor noi căi de monetizare și obținere de profit"; p. 77, 81.

[4] „BBC Micro Bit computer's final design revealed" 7.7.2015, http://www.bbc.com/news/technology-33409311(accessed 10.9.2015); „No assembler required: How to teach computer science in nursery school", The Economist, 1.8.2015.

[5] Niciuna din cele mai mari zece companii din sectorul tehnologiei în funcție de capitalizarea bursieră nu are sediul în UE (opt sunt companii din SUA, una din China și una din Taiwan), conform PWC Global Top Ten Companies by Market Capitalisation, actualizarea din 31 martie 2015.

[6] „Volumele mari de date se referă la creșterea exponențială în ce privește atât disponibilitatea, cât și utilizarea automatizată a informațiilor: acestea se referă la seturi de date digitale gigantice deținute de corporații, guverne și alte mari organizații, care sunt apoi analizate pe larg (de aici venind denumirea de analitică) cu ajutorul unor algoritmi computerizați"; Avizul 3/2013 al Grupului de lucru „Articolul 29" privind limitarea scopului. Într-un raport al Casei Albe din 2014, volumele mari de date erau descrise astfel: „capacitatea tehnologică tot mai mare de a reda, acumula și prelucra un volum de date tot mai mare, la o viteză și de o varietate tot mai mare", vezi Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President („Raportul Podesta"), mai 2014.

[7] Conform legislației UE, „datele cu caracter personal" sunt definite ca fiind „orice informație referitoare la o persoană fizică identificată sau identificabilă („persoana vizată"): o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale"; articolul 2 litera (a) din Directiva 95/46/CE. Această definiție este comparabilă în mare cu cele adoptate de Consiliul Europei în Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal (cunoscută și sub numele de Convenția 108) și în Ghidul OCDE privind protecția vieții private și fluxurile transfrontaliere de date cu caracter personal. Pentru o analiză amănunțită, vezi „Avizul 4/2007 al Grupului de lucru prevăzut la articolul 29 privind conceptul de date cu caracter personal", Grupul de lucru „Articolul 136".

[8] Vezi, de exemplu, discursul Președintei Comisiei Federale pentru Comerț a Statelor Unite din 2014: „Proliferarea dispozitivelor conectate, costurile în scădere vertiginoasă la colectarea, stocarea și prelucrarea informațiilor și capacitatea brokerilor de date și a altora de a combina date offline și online înseamnă că întreprinderile pot acumula practic cantități nelimitate de informații legate de consumatori și le pot stoca pe termen nedefinit. Cu ajutorul analiticii predictive, aceștia pot afla surprinzător de multe despre fiecare dintre noi din acestea"; Observațiile introductive ale Președintei CFC Edith Ramirez, „Big Data: A Tool for Inclusion or Exclusion?", Washington, DC 15 septembrie

2014. Conform afirmațiilor lui Sandy Pentland, „Fizica socială este o știință socială cantitativă ce descrie conexiuni fiabile, matematice între fluxul de informații și idei, pe de o parte, și comportamentul oamenilor, pe de altă parte... aceasta ne permite să prezicem productivitatea grupurilor mici, a departamentelor din cadrul întreprinderilor și chiar a unor orașe întregi". De acest lucru „este nevoie pentru a construi sisteme sociale mai bune" (p. 4, 7) și pentru a „permite (funcționarilor de stat, directorilor din domeniul industriei și cetățenilor) să folosească instrumentele stimulentelor din rețelele sociale pentru *a crea noi norme de comportament*" (p. 189) (italicele noastre); Pentland, *Social Physics: How Good Ideas Spread: The Lessons from a New Science*.

[9] Eurobarometrul special 431 privind protecția datelor, iunie 2015, și Studiul Pew Research Panel din ianuarie 2014 privind percepția publică a vieții private și a securității în Era post-Snowden. Conform unui studiu, o vizită obișnuită pe un singur site duce la colectarea datelor de către 56 de instanțe, conform afirmațiilor lui Julia Angwin *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012). Raportul Casei Albe din 2014 privind volumele mari de date arată că „puterea de calcul și sofisticarea fără precedent... creează o asimetrie de putere între cei care dețin datele și cei care le furnizează intenționat sau din neatenție"; „unele dintre cele mai mari dificultăți descoperite cu ocazia acestei verificări se referă la modul în care analitica volumelor mari de date ar putea... crea un mediu decizional atât de opac încât autonomia individuală să se piardă într-un set de algoritmi impenetrabili".

[10] Cu ajutorul datelor anonime publice ale recensământului din 1990, 87% din populația SUA ar putea fi identificată după codul lor poștal format din cinci cifre combinat cu sexul și data nașterii; vezi Paul Ohm „Broken promises of privacy: responding to the surprising failure of anonymisation", UCLA Law Review 2010, și „Record linkage and privacy: issues in creating new federal research and statistical info", aprilie 2011. ADN-ul este unic (cu excepția gemenilor identici) și stabil pe toată durata vieții. Acesta conține informații legate de etnie, predispoziții la boli și poate identifica alți membri ai familiei. În ianuarie 2013, cercetătorii au fost capabili să identifice persoanele și familiile pe baza datelor ADN obținute din baze de date genealogice făcute publice; Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. & Erlich, Y. *Science* 339, 321–324 (2013). Vezi și „Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts", 23.6.2014 http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/ (accesat la 10.9.2015). Vezi și Avizul 04/2007 al Grupului de lucru „Articolul 29" privind conceptul de date cu caracter personal; Avizul 03/2013 al Grupului de lucru „Articolul 29" privind limitarea scopului; Avizul 06/2013 al Grupului de lucru „Articolul 29" privind reutilizarea datelor deschise și a informațiilor din sectorul public; și Avizul 05/2014 al Grupului de lucru „Articolul 29" privind asigurarea anonimatului.

[11] Sursa: Gartner.

[12] Vezi de exemplu discuția de grup „Care este viitorul statisticilor oficiale în era volumelor mari de date?" the Royal Statistical Society, Londra, 19 ianuarie 2015; http://www.odi.org/events/4068-future-official-statistics-big-data-era (accesat la 10.9.2015).

[13] Ten technologies which could change our lives: potential impacts and policy implications, Scientific Foresight Unit, Serviciul de Cercetare al Parlamentului European, ianuarie 2015.

[14] Programul de lucru al UE Orizont 2020 pentru anii 2016-2017 susține aceste evoluții, inclusiv proiecte-pilot pe scară largă care vor avea preocupări legate de viața privată și de etică.

[15] Asigurarea a fost descrisă ca „modelul de afaceri nativ pentru internetul obiectelor"; „From fitness trackers to drones, how the 'Internet of Things' is transforming the insurance industry", Business Insider 11.6.2015. Noțiunea discriminării prin preț în dreptul concurenței, derivată din articolul 102 din TFUE, care interzice o întreprindere dominantă pe o piață prin „impunerea, direct sau indirect, a prețurilor de vânzare sau de cumpărare sau a altor condiții de tranzacționare inechitabile", este deosebit de discutabilă; vezi, de exemplu, Damien Gerardin și Nicolas Petit Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles (July 2005), Global Competition Law Centre, Seria de documente de lucru nr. 07/05. În ceea ce privește volumele

mari de date şi potenţialul acestora (conform autorilor, nerealizat încă) de a accelera stabilirea de preţuri personalizate, vezi Biroul Executiv al Preşedintelui Statelor Unite, Big Data and Differential Pricing, februarie 2015, şi o analiză recentă ce concluzionează că preţurile personalizate atrag după sine în general prelucrarea datelor cu caracter personal şi, prin urmare, trebuie să respecte principiul transparenţei prevăzut în legea privind protecţia datelor, care prevede ca întreprinderile să informeze oamenii despre scopul prelucrării datelor lor cu caracter personal: întreprinderile trebuie să spună dacă personalizează preţurile. De asemenea, dacă o întreprindere foloseşte un modul cookie pentru a recunoaşte pe cineva, Directiva privind confidenţialitatea în mediul electronic prevede ca întreprinderea să informeze persoana despre scopul acelui modul cookie; schiţă de lucru de Frederik Borgesius „Online Price Discrimination and Data Protection Law". Disponibilă la http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (accesat la 10.09.2015).

[16] Dispozitivele medicale sunt definite în dreptul UE în temeiul Directivei 93/42/CEE a Consiliului privind dispozitivele medicale, modificată prin Directiva 2007/47/CE a Parlamentului European şi a Consiliului din 5 septembrie 2007. În ceea ce priveşte implicaţiile „sănătăţii mobile" asupra protecţiei datelor, vezi avizul 1/2015 al AEPD.

[17] Conform Eurostat, 21% dintre persoanele fizice şi 19% dintre persoanele juridice din UE folosesc servicii de stocare de tip cloud.

[18] „Dacă internetul din lumea întreagă ar fi o ţară, aceasta ar fi a 12-a cea mai mare consumatoare de electricitate din lume, situată undeva între Spania şi Italia. Aceasta reprezintă aproximativ 1,1-1,5 la sută din consumul global de electricitate (la nivelul anului 2010) şi din gazele cu efect de seră generate anual de 70-90 dintre marile (500 MW) termocentrale electrice alimentate cu cărbune". Consiliul de Apărare a Resurselor Naturale, Evaluarea eficienţei centrelor de date: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers 2014.

[19] Raportul studiului „SMART 2013/0043 - Uptake of Cloud in Europe".

[20] Sursa: Eurostat.

[21] Termenul „economie de partajare" a fost criticat drept înşelător: „The Sharing Economy Isn't About Sharing at All", Giana M. Eckhardt şi Fleura Bardhi, Harvard Business Review, 28.01.2015.

[22] Rachel Botsman şi Roo Rogers, *What's Mine Is Yours: How Collaborative Consumption is Changing the Way We Live*, 2011.

[23] Future of Privacy Forum, „User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy", iunie 2015.

[24] Vezi atelierul din 9 iunie 2015 al Comisiei Federale pentru Comerţ a SUA privind „Concurenţa, protecţia consumatorului şi probleme economice ridicate de economia bazată pe partajare", https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/ (accesat la 10.09.2015).

[25] Referitor la implicaţiile dronelor sau ale sistemelor aeronautice pilotate de la distanţă asupra protecţiei datelor, vezi avizul AEPD privind Comunicatul de la Comisie către Parlamentul European şi Comisie privind „O nouă eră pentru aviaţie - Deschiderea pieţei aviatice pentru utilizarea sigură şi sustenabilă de către civili a sistemelor aeronautice pilotate de la distanţă", noiembrie 2014.

[26] Sursa: Boston Consulting Group.

[27] Gartner.

[28] Algoritmul de recunoaştere facială DeepFace de la Facebook a raportat un succes de 97% - depăşind oamenii; DeepFace: Closing the Gap to Human-Level Performance in Face Verification, publicat în raportul privind Conferinţa IEEE privind vederea artificială şi recunoaşterea formelor, iunie 2014.

[29] Robo a fost definit ca o „mașină situată în lume care simte, gândește și acționează”; Bekey, G, Tendințe actuale în robotică: tehnologie și etică, în Robot Ethics - The ethical and social implications of robotics, The MIT Press2, 2012, pag. 18. Se estimează că 22 000 de roboți vor fi vânduți în perioada 2013-2016; Raportul IRF World Robotics, 2013. Referitor la inteligența artificială, vezi Rise of the Machines, Economist, 09.5.15 și Pew Research Centre Internet Project 2014. O întreprindere de inteligență artificială s-a lăsat cumpărată de către o companie tehnologică de top în anul 2014 cu condiția formării unui consiliu de etică și siguranță și a interzicerii utilizării lucrărilor din domeniul inteligenței artificiale în scopuri militare și de servicii secrete; Forbes, Inside Google's Mysterious Ethics Board, 3.2.2014.

[30] Pentland, *Social physics*, p. 147.

[31] Vezi nota 9 de mai sus. Pentland *Social Physics* p. 153: „Mari salturi în sectorul sănătății, transport, energie și securitate sunt desigur posibile... principalele bariere în calea atingerii acestor obiective sunt preocupările pentru viața privată și faptul că nu am ajuns încă la niciun consens referitor la schimburile între valorile personale și cele sociale”. Dezbaterea din jurul pandemiei de Ebola din anul 2014 din Africa de Vest este exemplificativă pentru modul în care apare această falsă dicotomie între nevoile de intimitate individuală și nevoile sociale. Tendința a fost ca bolile să fie urmărite și durata lor măsurată prin studii și recensăminte a căror valabilitate expiră foarte ușor și care sunt greu de extrapolat pentru a anticipa unde vor lovi bolile data viitoare. Există câteva exemple de utilizare a volumelor mari de date pentru a urmări izbucnirea epidemiilor de malarie în Namibia și Kenya, iar în 2009 pentru a urmări eficiența avertismentelor guvernamentale privind sănătatea în timpul crizei de gripă porcină din Mexic. O sursă de date ar fi înregistrările convorbirilor telefonice mobile, care arată stația de bază care a asigurat convorbirea și poate da în timp real o aproximare brută a locației persoanelor și a direcției în care se îndreaptă. Strângerea acestor înregistrări nu este una țintită - adică nu poate face diferența între persoanele care au și care nu au Ebola. O organizație non-profit suedeză a cartografiat mobilitatea populației în Africa de Vest, însă datele nu au fost folosite deoarece operatorii de telefonie mobilă nu au vrut să le divulge cercetătorilor externi autorizați, susținând că au nevoie de instrucțiuni de la guverne, care, la rândul lor, au invocat preocupări pentru viața privată ce nu au putut fi garantate prin dreptul UE; http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola. (accesat la 10.09.2015)

[32] Avizul AEPD 3/2015.

[33] Ipoteza volumelor mari de date că „N=toți” se referă la a privi în ansamblu toate punctele de date, nu doar o mostră din acestea, Viktor Mayer-Schönberger și Kenneth Cukier, *The Rise of Big Data: How it's changing the way we think about the world*, 2013. Consiliul de la Lisabona și Institutul pentru politici progresive au argumentat că prosperitatea va crește prin maximizarea „densității digitale” - „cantitatea de date folosite pe cap de locuitor într-o economie” http://www.lisboncouncil.net/component/downloads/?id=1178 (accesat la 10.09.2015). Grupul de lucru internațional privind protecția datelor în telecomunicații (cunoscut sub numele de „Grupul de la Berlin”) a propus derogări pentru volumele mari de date de la principiile de protecție a datelor; http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf. (accesat la 10.09.2015). Forumul Economic Mondial a cerut ca accentul să fie pus pe utilizare, nu pe colectare și să se renunțe la cerința acordului pentru colectarea datelor personale; Unlocking the Value of Personal Data: From Collection to Usage, 2013.

[34] Vezi Avizul preliminar al AEPD privind Confidențialitatea și competitivitatea în era volumelor mari de date.

[35] Articolul 21 din Carta drepturilor fundamentale interzice „Orice discriminare pe bază de sex, origine rasială, culoare, origine etnică sau socială, caracteristici genetice, limbă, religie sau convingeri, opinii politice sau de orice altă natură, apartenență la o minoritate națională, avere, naștere, handicap, vârstă sau orientare sexuală”. Multe dintre aceste categorii de date („care dezvăluie originea rasială sau etnică, opiniile politice, credințele religioase sau filosofice, apartenența sindicală,

precum și prelucrarea datelor privind sănătatea sau viața sexuală") beneficiază de protecție sporită în baza articolului 8 din Directiva 95/46/CE.

[36] Referitor la ideea unui fond comun digital, vezi Ambition numérique: Pour une politique française et européenne de la transition numérique, Consiliul Digital Francez, iunie 2015 pag. 276; Bruce Schneier susține înființarea de „spații publice fără proprietar" pe internet, cum sunt parcurile publice, *Data and Goliath*, pag. 188-189; Sandy Pentland aduce argumente pentru un „fond comun de date publice", *Social Physics*, pag. 179. Referitor la estimarea siguranței de publicare a unor seturi de date agregate precum datele deschise, vezi Avizul 06/2013 al Grupului de lucru „Articolul 29" privind reutilizarea datelor deschise și a informațiilor din sectorul public.

[37] „Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent" http://crackedlabs.org/studie-kommerzielle-ueberwachung/info. Referitor la transparența calificată, vezi de ex. Frank Pasquale: *The Black Box Society: The Secret Algorithms that Control Money and Information*.

[38] „În spatele tehnologiei ce afectează relațiile sociale se află aceleași relații sociale", David Noble, „Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools", în *Case Studies in the Labor Process*, ed. Andrew Zimbalist, 1979. Vezi și Judy Wacjman, *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014 p. 89-90; și Zuboff, „Big Other" (citate în nota 3 de mai sus).

[39] Avizul 05/2014 privind tehnicile de asigurare a anonimatului, adoptat la data de 10 aprilie 2014 (Grupul de lucru „Articolul 216").

[40] Referitor la scutirea interpretată restrictiv de la regulile de protecție a datelor în scopuri pur personale sau gospodărești, vezi hotărârea CJUE în cauza C-212/13 *František Ryneš împotriva Úřad pro ochranu osobních údajů.*

[41] Termenul de prosumator a fost inventat de Alvin Toffler în *The Third Wave*, 1980. Pentru o discuție legată de „mediul prosumatorului" și de modul în care ar trebui reglementată, vezi Ian Brown și Chris Marsden, *Regulating Code*, 2013.

[42] Avizul Grupului european pentru etică în domeniul științei și al noilor tehnologii pentru Comisia Europeană: Etica tehnologiilor de securitate și supraveghere, Avizul nr. 28, 20.5.2015, p. 74.

[43]Vezi, de exemplu, Homer Economicus: The Simpsons and Economics, ed. Joshua Hall, 2014.

[44] Conform celei mai conservatoare definiții a greșelii, acest lucru înseamnă că 23 de milioane de americani au erori semnificative într-un raport de consumator. Cinci la sută dintre participanții la studiu avea erori care, odată corectate, le-au îmbunătățit scorul de credit în așa măsură încât au putut obține credit la un preț mai scăzut; Comisia Federală pentru Comerț, Raport către Congres conform Secțiunii 319 din Legea tranzacțiilor de credit echitabile și corecte din 2003, decembrie 2012; Chris Jay Hoofnagle, How the Fair Credit Reporting Act Regulates Big Data (10 septembrie 2013). Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet, 2013. Disponibil pe site-ul SSRN: http://ssrn.com/abstract=2432955.

[45] Forumul Economic Mondial afirmă că datele sunt un activ valoros al persoanei fizice ale cărei drepturi de posesie, utilizare și dispoziție poate fi acordat întreprinderilor și guvernelor în schimbul unor servicii. Vezi discursurile recente, precum și discursul Vicepreședintelui Comisiei, dl Ansip, de exemplu, la data de 7.9.2015, la reuniunea anuală de la Bruegel, intitulat „Productivitate, inovație și digitalizare - care politică globală ridică probleme?": „Proprietatea și administrarea fluxurilor de date, utilizarea și reutilizarea datelor. Administrarea și stocarea datelor. Acestea susțin sectoare emergente importante precum tehnologia de tip cloud computing, internetul obiectelor și volumele mari de date".

[46] „Așadar cine deține dreptul de a folosi informațiile și datele care nu aparțin cu adevărat sieși? Aceasta este o problemă care transcende limitele comerțului, eticii și moralei, ducând la probleme de confidențialitate și protecția vieții private"; Al-Khouri Nov 2012, http://www.academia.edu/6726887/Data_Owner

ship Who Owns My Data 036. Vezi și Margaret Jane Radin, Incomplete Commodification in the Computerized World, in The Commodification of Information 3, 17, Niva Elkin-Koren & Neil Weinstock Netanel eds. 2002: „Este o mare diferență dacă viața privată este văzută ca un drept al omului, care este legat de persoane în virtutea personalității lor, sau ca un drept de proprietate, ceva ce poate fi deținut și controlate de persoane. Drepturile omului se presupune că sunt inalienabile pe piață, în timp ce drepturile de proprietate se presupune că sunt alienabile pe piață".

[47] Proiectul Crosscloud al MIT Computer Science and Artificial Intelligence Lab, susținut de câteva întreprinderi situate în UE, își propune „1) să faciliteze dezvoltarea de software multi-utilizator (social) folosind numai dezvoltarea front-end și respectând drepturile și viața privată a utilizatorilor. și 2) să le ofere utilizatorilor libertatea de a se muta cu ușurință între aplicații, între platforme și între rețelele sociale, păstrându-și datele și legăturile sociale"; http://openpds.media.mit.edu/#architecture (accesat la 10.9.2015).

[48] Vezi explicația la articolul 1 din Carta drepturilor fundamentale.

[49] Martha Nussbaum, Objectification, in Philopsophy and Public Affairs 24, 4, 1995.

[50] Hotărârea din 15 decembrie 1983, BVerfGE 65, 1-71, Volkszählung.

[51] Vezi Grupul european pentru etică în domeniul științei și al noilor tehnologii, Aviz asupra eticii și supravegherii, p. 75. Un studiu a sugerat că un algoritm ce viza reclamele era discriminator, cu căutări care returnau în medie anunțuri pentru locuri de muncă mai bine plătite pentru bărbați comparativ cu femeile care vizitau site-urile de locuri de muncă; Universitatea Carnegie Mellon și Institutul Internațional de Informatică. Referitor la tendința asistenților digitali de a avea din oficiu o voce feminină, vezi de exemplu Judy Wajcman, Feminist theories of technology. Cambridge Journal of Economics, 34 (1). pag. 143-152, 2010.

[52] Giorgio Agamben, *State of Exception, 2005.*

[53] Neil Richards, Neil și Jonathan King, Big Data Ethics (19 mai 2014), Wake Forest Law Review, 2014.

[54] BBC, Organul de supraveghere a informațiilor investighează „charity data sales", 1.9.2015.

[55] Vezi scrisoarea de la Future of Life Institute. Enciclica papală *Laudato Si:* „când mijloacele de comunicare în masă și lumea digitală devin omniprezente, influența lor poate opri oamenii de la a învăța cum să trăiască înțelept, cum să gândească profund și cum să iubească cu generozitate. În acest context, marii înțelepți din trecut își asumă riscul de a rămâne neauziți în mijlocul zgomotului și distragerii cauzate de un exces de informații. Trebuie făcute eforturi pentru a ajuta aceste medii să devină surse de noi progrese culturale pentru umanitate, nu o amenințare pentru cele mai profunde bogății ale noastre. Adevărata înțelepciune, ca prim fruct de autoanaliză, dialog și întâlnire generoasă între persoane, nu este dobândită printr-o simplă acumulare de date care duce în final la supraîncărcare și confuzie, un fel de poluare mentală. Adevăratele relații cu ceilalți, cu toate complicațiile aferente, tind acum să fie înlocuite cu un tip de comunicare prin Internet care ne permite să alegem sau să eliminăm relațiile după pofta inimii, dând astfel naștere unui nou tip de emoție născocită, care are de-a face mai mult cu dispozitivele decât cu ceilalți oameni și cu natura. Mijloacele de comunicare în masă din zilele noastre ne permit într-adevăr să comunicăm și să ne împărtășim cunoștințele și afecțiunile. Totuși, uneori ele ne și împiedică să intrăm în contact direct cu durerea, cu fricile și bucuriile celorlalți și cu complexitatea experiențelor lor personale. Din acest motiv, ar trebui să ne preocupe faptul că, odată cu posibilitățile interesante oferite de aceste mijloace, poate apărea și o profundă și melancolică nemulțumire față de relațiile interpersonale sau un dăunător sentiment de izolare".

[56] Vezi Acțiunea 4 din Strategia AEPD 2015-2020, dezvoltarea unei dimensiuni etice pentru protecția datelor.